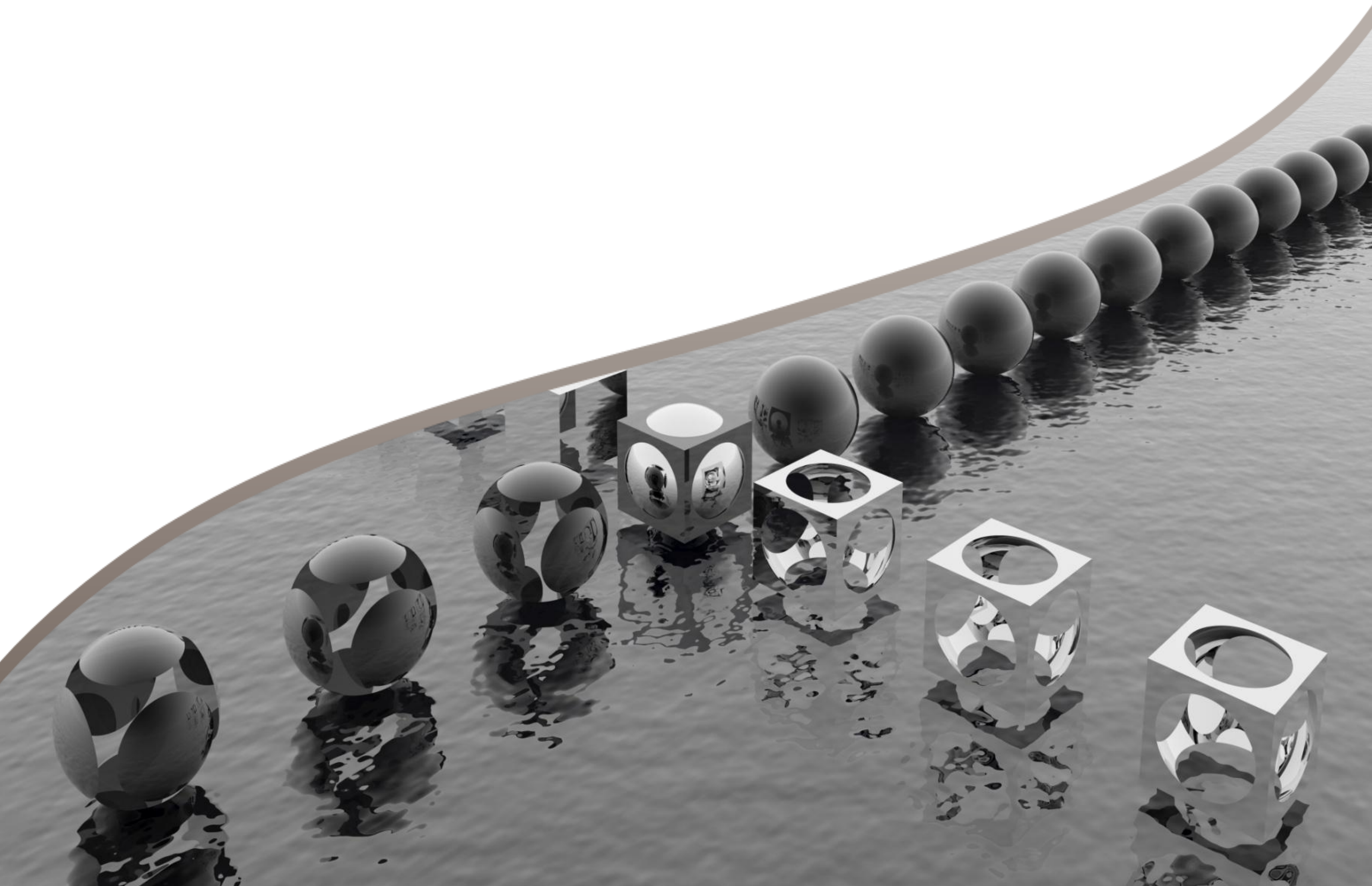
Beleidsdoorlichting Art. 25.2

Veiligheid, Informatie en Technologie

in opdracht van het Ministerie van Veiligheid en Justitie



Capgemini Consulting

Auteurs:
Drs. E.P. Hoorweg MCM
Drs. M.C.A.B. Hols
B.T. Bikkers MSc

Datum:

April 2013

Referentienummer:

13.0144

Capgemini Consulting

Inhoud

1 Inleiding

1.1 Doel en vraagstelling

Conform artikel 20 van de Comptabiliteit Wet dient alle beleid periodiek te worden geëvalueerd. Leidraad voor de uitvoering van een beleidsdoorlichting vormt de Regeling periodiek evaluatieonderzoek en beleidsinformatie 2006 (verder: RPE 2006)[1]. Dit rapport geeft de uitkomsten weer van de beleidsdoorlichting die is verricht in opdracht van het ministerie van Veiligheid en Justitie op de volgende operationele beleidsdoelstelling:

"Het bevorderen van efficiënt en effectief gebruik van communicatie, informatie en technologie door de veiligheidspartners".

Deze operationele beleidsdoelstelling is opgenomen in artikel 25.2 van de begroting 2012 van het ministerie van Veiligheid en Justitie.

Een beleidsdoorlichting is 'een evaluatie van beleid op het niveau van de algemene of operationele doelstellingen'. Een beleidsdoorlichting bestaat uit in ieder geval de volgende onderdelen[2]:

a) Beschrijving en analyse van het probleem dat aanleiding was voor het beleid;
b) Beschrijving en motivering van de rol van de rijksoverheid;
c) Beschrijving van de onderzochte beleidsdoelstellingen;
d) Beschrijving van de gehanteerde instrumenten en analyse van de maatschappelijke effecten ervan;
e) Beschrijving van de budgetten die zijn ingezet.

Het ministerie van Veiligheid en Justitie heeft Capgemini Consulting gevraagd om de beleidsdoorlichting uit te voeren voor het artikel 25.2 uit de beleidsbegroting 2012. De beleidsdoorlichting dient daarbij de periode 2007 tot en met 2012 te bestrijken. In deze periode (1 oktober 2010) is de verantwoordelijkheid voor de betreffende beleidsdoelstelling overgegaan van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties naar het ministerie van Veiligheid en Justitie. In de periode voor 1 oktober 2010 maakte de betreffende beleidsdoelstelling onderdeel uit van een groter geheel, te weten artikel 4 van de beleidsbegroting van het ministerie van BZK. De beleidsdoorlichting dient uitdrukkelijk te beperken tot de scope van het huidige artikel 25.2. In hoofdstuk drie van deze rapportage is de ontwikkeling van de beleidsdoelstelling en de onderliggende instrumenten nader toegelicht.

1 Per 1 januari 2013 is de RPE vernieuwd. Aangezien echter de doorlichting is gestart in 2012, is daarvoor nog de RPE 2006 gehanteerd.

2 Regeling periodiek evaluatieonderzoek en beleidsinformatie 2006, ministerie van Financiën 18 april 2006. Aan deze onderdelen zijn vervolgens tien vragen verbonden. Deze zijn opgenomen in bijlage D.

1.2 Uitgangspunten beleidsdoorlichting

Voor deze beleidsdoorlichting zijn de volgende uitgangspunten gehanteerd:

- De beleidsdoorlichting heeft als doel om te leren van de opzet en werking van het instrument;
- Zowel een terugblik als een korte vooruitblik maken deel uit van de beleidsdoorlichting;
- De beleidsdoorlichting is zoveel mogelijk gebaseerd op onafhankelijke (deel)onderzoeken naar de doelmatigheid en doeltreffendheid van het beleid en vormt daarmee geen ex-post evaluatie op zichzelf;
- Het onderzoek is uitgevoerd door een onafhankelijke partij (Capgemini Consulting).

Het onderzoek is begeleid door een begeleidingscommissie vanuit het ministerie van Veiligheid en Justitie[3] met vertegenwoordiging uit DGPol, NCTV en het WODC.

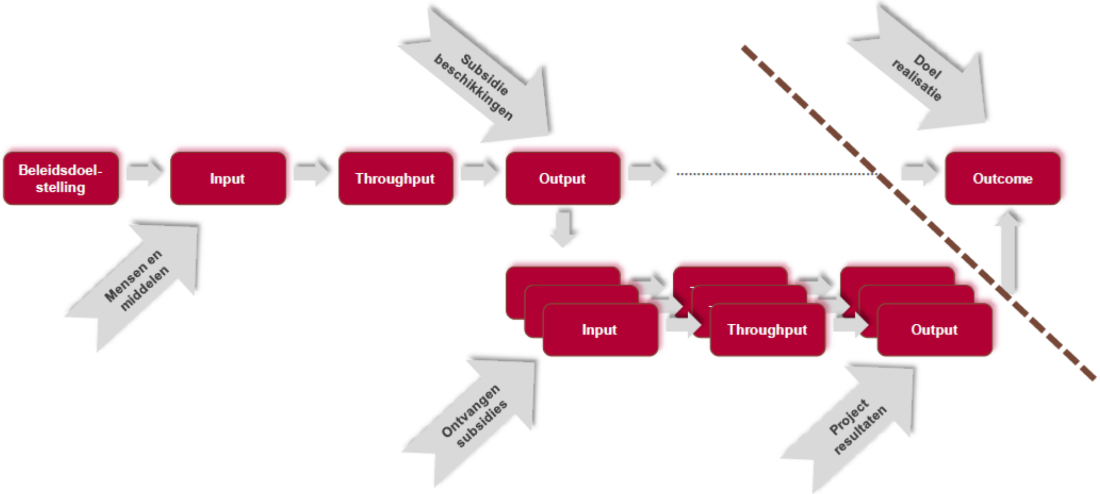
1.3 Aanpak onderzoek

De beleidsdoorlichting is tot stand gekomen op basis van literatuuronderzoek, documentanalyse en interviews. Waar informatie vanuit documenten of literatuur niet voorhanden was, zijn aanvullende inzichten verzameld aan de hand van semigestructureerde interviews met betrokken functionarissen[4]. Deze interviews schetsen een beeld van ervaringen met het bevorderen van efficiënt en effectief gebruik van communicatie, informatie en technologie door de veiligheidspartners, maar representeren geen 'objectieve waarheid'. In de rapportage is aangegeven waar bevindingen voortkomen uit literatuuronderzoek en waar het een algemeen beeld uit aanvullende interviews betreft. De beleidsdoorlichting is uitgevoerd in de periode november 2012 tot maart 2013.

De vijf onderdelen van de beleidsdoorlichting (zie paragraaf 1.1) zijn geanalyseerd en beschreven aan de hand van het volgende referentiekader:

[3] Zie bijlage A voor de samenstelling van de begeleidingscommissie.

[4] Een overzicht van geïnterviewde personen is opgenomen in bijlage B.



Onderdelen 'a, b en c' richten zich op de beleidsdoelstelling zelf in termen van aanleiding, verantwoordelijkheid en beschrijving van de betreffende doelstelling. Onderdeel 'd' richt zich op de beschrijving van de instrumenten die zijn ingezet om de beleidsdoelstelling te realiseren en de effecten die hieruit zijn voortgekomen. Voor dit onderdeel is het van belang om onderscheid te maken in 'output' en 'outcome'. De output is het resultaat van een beleidsinstrument waarbij sprake is van een direct causaal gevolg. De output is daarmee ook volledig beïnvloedbaar door degene die de instrumenten inzetten. Bij beleidsdepartementen bestaat de output veelal uit subsidiebeschikkingen of doeluitkeringen aan uitvoeringsorganisaties. De output (een beschikking) vormt vervolgens de input voor de uitvoeringsorganisatie. Met deze input realiseert de uitvoeringsorganisatie activiteiten die weer leiden tot nieuwe resultaten (output). Het totaal van de output van uitvoeringsorganisaties leidt tot een maatschappelijk effect (outcome). Dit maatschappelijk effect wordt echter vaak verstoort door andere (niet beïnvloedbare – exogene) factoren waardoor sprake is van een plausibiliteitrelatie. In het kader van de beleidsdoorlichting is het derhalve van belang of het aannemelijk is dat de output heeft bijgedragen aan het beoogde maatschappelijk effect.

De mate waarin de realisatie van zowel de output als de outcome is vast te stellen, hangt mede af van de prestatie-indicatoren die voor de betreffende beoogde resultaten zijn opgenomen. Indien geen prestatie-indicatoren zijn opgenomen dan krijgt de vaststelling een meer kwalitatief karakter. Conform de RPE 2006 is een beleidsdoorlichting zo veel mogelijk gebaseerd op reeds eerder uitgevoerde evaluaties.

1.4 Leeswijzer

Dit rapport is als volgt opgebouwd:

- In hoofdstuk twee zijn de achtergronden en aanleiding van het bevorderen van efficiënt en effectief gebruik van communicatie, informatie en technologie door de veiligheidspartners toegelicht. Daarnaast is ingegaan op de verantwoordelijkheid van de overheid voor deze beleidsdoelstelling.
- In hoofdstuk drie zijn de beleidsdoelstelling en de bijbehorende beleidsinstrumenten nader beschreven. Vervolgens is per beleidsinstrument toegelicht hoe deze in de periode tussen 2007 en 20012 zijn gerealiseerd.
- In hoofdstuk vier zijn de budgetten behorende bij de beleidsdoelstelling 25.2 geanalyseerd en toegelicht.
- In hoofdstuk vijf bevat een samenvatting en de belangrijkste conclusies van de beleidsdoorlichting.

2 Achtergrond

2.1 Inleiding

In dit hoofdstuk is ingegaan op de achtergrond die ertoe heeft geleid dat artikel, wat ingaat op het bevorderen van efficiënt en effectief gebruik van communicatie, informatie en technologie door de veiligheidspartners, tot stand is gekomen. Hiertoe wordt eerst de maatschappelijke context van dat moment geschetst (§2.2). Vervolgens wordt ingegaan op het probleem dat de aanleiding was voor het artikel en op de oorzaken van dat probleem (§2.3). Ten slotte wordt de verantwoordelijkheid van de overheid daarbij beschreven (§2.4).

2.2 Maatschappelijke context: streven naar samenwerking en innovatie

Het jaar 2007 wordt gekenmerkt door de overgang van het kabinet Balkenende III naar Balkenende IV. Nederland. In haar beleidsprogramma 2007-2011wordt onder pijler 5 aandacht besteed aan veiligheid[5]. De missie van deze pijler 5 is als volgt beschreven: "*We willen een samenleving waarin mensen zich veilig, vertrouwd en met elkaar verbonden voelen. Een samenleving waarin wederzijds respect de norm is, waarin we elkaar geen overlast bezorgen en waarin geweld een uitzondering is, net als diefstal, vernieling en andere vormen van criminaliteit. Zo'n samenleving kan alleen worden bereikt als het streven daarnaar breed wordt omarmd, niet alleen in woorden maar ook in daden. Burgers en ondernemingen kunnen daarin veel betekenen op grond van hun eigen verantwoordelijkheid. Van de overheid mag worden verwacht dat zij weet op te treden wanneer de veiligheid in de knel komt. Alleen dan is onze samenleving een rechtsstaat in de volle zin van het woord".*

Veiligheid werd aldus gezien als een van de basisbehoeften van de samenleving. Via pijler 2 van het beleidsprogramma onderkende het nieuwe kabinet de kansen die technologische innovatie biedt voor veiligheidsvraagstukken. In pijler 2 werd daarom de ambitie neergelegd om te komen tot een maatschappelijke innovatieagenda voor Veiligheid.

Nederland werd op dat moment geconfronteerd met een veiligheidssituatie die sterk in beweging is[6]. De veiligheidssituatie en de beleving daarvan werd beïnvloed door:

- De opkomst van internationale criminaliteit en terrorisme. Het samenwerken met de USA, de veelheid aan internationale organisaties die in Nederland zijn gevestigd en de spilrol die Nederland speelt in financiële, logistieke en personele stromen, maken Nederland een potentieel doelwit;
- De sterke toename van aantal, aard aanleiding en uitwerking van zowel security als safety incidenten, waarbij de kwetsbaarheid van onze maatschappij zowel op collectief niveau als individueel niveau steeds groter wordt;
- Een sterke toename van complexe risico's door intensief ruimtegebruik en de integratie van woon-, werk-, transport- en recreatieactiviteiten;

[5] Beleidsprogramma Kabinet Balkenende IV 2007-2011 "Samen werken samen leven", juni 2007.

[6] Maatschappelijke Innovatie Agenda Veiligheid, bijlagen, juni 2008.

- Europese samenwerking en regelgeving op het gebied van terreur-, criminaliteits- en calamiteitbestrijding speelt Europese regelgeving in toenemende mate een rol;
- Snelle technologische ontwikkelingen: de ontwikkelingen op het gebied van onder andere de communicatietechnologie hebben gezorgd voor globalisering en flexibilisering van de maatschappij. Zowel "specialistische" technologie als "consumenten" technologie zijn op grote schaal beschikbaar voor criminele en terroristische groeperingen;
- Door de samenstelling van de Nederlandse bevolking en de toenemende radicalisering is Nederland in toenemende mate kwetsbaar voor deelname aan internationale conflicten van politieke, nationale en religieuze aard;
- Er worden successen geboekt (terugdringen criminaliteit en overlast) maar die vertalen zich lang niet altijd in een veiliger gevoel bij de burger.

In de probleemanalyse van het beleidsprogramma Balkenende IV (pijler 5) geeft het kabinet aan dat de overheidsorganisatie verder op orde moet worden gebracht. Doelstelling 5.7 richt zich derhalve op een effectieve organisatie van de veiligheidsketen: "*Samenwerkingsverbanden binnen de organisatie van de veiligheid worden versterkt met betrokkenheid van de burger*". Dit streven naar betere samenwerking (en daarmee het geconstateerde gebrek er aan tot 2007) is kenmerkend voor het veiligheidsdomein in deze periode. Daarbij gaat het niet alleen om samenwerking *tussen* organisaties maar ook om samenwerking *binnen* organisaties van het veiligheidsdomein.

Veiligheid is een verantwoordelijkheid van een veelheid aan (semi)publieke en private organisaties; Politie, brandweer, ambulancediensten, marechaussee, centrale overheid, gemeenten en bedrijven. Kenmerkend voor deze partners in veiligheid is hun autonomie in het nemen van beslissingen aangaande informatiebeleid en ICT.

De politie is in deze periode georganiseerd in 25 regiokorpsen (en één landelijke dienst). Het beheer van de politie ligt weliswaar bij het ministerie van BZK maar het bevoegd gezag is een primair lokale/regionale aangelegenheid (korpsbeheerder en officier van justitie). In de periode 2007, 2008 wordt gediscussieerd over aanpassing van het politiebestel. In samenspraak met de korpsbeheerders zijn in 2007 samenwerkingsafspraken geformuleerd waaraan de politie eind 2008 moet voldoen. Daarbij wordt een belangrijk deel gevormd door afspraken op het gebied van ICT.

De brandweer is in deze periode nog sterk decentraal georganiseerd en valt onder het lokaal bestuur waarbij in een rapport van de IOOV wordt geconcludeerd dat de gemeentebesturen een beperkte belangstelling hebben voor de brandweerzorg; "*Ondanks veranderende maatschappelijke omstandigheden is hervorming van het brandweerbestel in de vorm van regionalisering niet of nauwelijks van de grond gekomen*"[7]. Het kabinet streeft naar volledige regionalisering (25) van de brandweer door het afsluiten van meerjarige convenanten. Daarmee komt de brandweer onder verlengd lokaal bestuur.

De Wet op de Veiligheidsregio's (Wvr) ligt in 2007 ter behandeling in de Tweede Kamer. Deze wet streeft naar een hogere kwaliteit en onderlinge (multidisciplinaire) samenwerking tussen politie, brandweer en GHOR en is van kracht per 1 oktober 2010.

[7] Bestuurlijke aansturing van de brandweerzorg. IOOV december 2006.

2.3 Aanleiding tot de operationele beleidsdoelstelling

Politie, brandweer, ambulancediensten, marechaussee, centrale overheid, gemeenten en bedrijven hebben ieder een verantwoordelijkheid in het handhaven van de openbare orde en veiligheid. Om de veiligheid van burgers te kunnen waarborgen is het noodzakelijk dat deze partners in veiligheid goed met elkaar samenwerken, zowel lokaal, regionaal, nationaal als internationaal, zodat er minder slachtoffers en schade optreden en de veiligheid van hulpverleners beter kan worden gewaarborgd[8]. Goede samenwerking vraagt om goede informatie-uitwisseling. Goede informatie-uitwisseling vraagt om gedeelde informatievoorzieningen die deze uitwisseling mogelijk maakt. In 2004 werd reeds geconstateerd dat de informatievoorziening ten behoeve van rampenbestrijding onvoldoende op orde was[9]. Daarom is in 2005 de ACIR – Adviescommissie Coördinatie ICT Rampenbestrijding – ingesteld. De ACIR heeft geconstateerd dat de knelpunten in de informatievoorziening veelal een achterliggende oorzaak hebben in de bestuurlijk/financiële en organisatorische context. Door de toenmalige constellatie van veel nevengeschikte besturen en een bestuurscultuur van consensus was het moeilijk om te komen tot een samenhangende informatiehuishouding van de partners in veiligheid. Op basis van haar analyse van knelpunten en achterliggende oorzaken deed de ACIR drie aanbevelingen:

1. Uniformeer de informatievoorziening landelijk;
2. Borg informatiemanagement bestuurlijk en operationeel op tenminste regionaal niveau;
3. Organiseer een stok achter de deur om besluitvorming af te dwingen, indien eenduidigheid achterwege blijft.

De Inspectie OOV rapporteert in 2008 op basis van de ADR (periode 2003-2007) dat verbeterpunten zich manifesteren in de voorbereiding op de kritische processen zoals informatiemanagement, leiding en coördinatie en opschaling. Ook uit toenmalige bestuurlijke rapportages van de Commissarissen van de Koningin blijkt een behoefte aan versterking van het informatiemanagement en een landelijk uniform systeem. De minister geeft daarbij aan een groot voorstander te zijn van uniformering; "*in het Besluit veiligheidsregio's neem ik eisen aan informatiemanagement op die deze uniformering mogelijk maakt*"[10].

In een maatschappelijke context waarin het kabinet Balkenende IV streeft naar (bestuurlijke) samenwerking in het veiligheidsdomein, er een gebrek wordt geconstateerd aan goede informatie-uitwisseling en wordt gezocht naar toepassing van innovatieve technologieën om de veiligheid te vergroten, wordt in 2007 de algemene beleidsdoelstelling geformuleerd: "*Goed samenwerkende partners in veiligheid*". Deze beleidsdoelstelling heeft zich geëvolueerd tot de volgende formulering in 2012: "*Een veiliger samenleving door de bestuurlijke kracht van de decentrale overheden en hun partners in veiligheid te versterken".* Deze algemene doelstelling is gedeeld in twee operationele doelstellingen:

- 25.1 De veiligheidspartners in staat stellen om hun werk efficiënt en effectief uit te kunnen oefenen;
- 25.2 Het bevorderen van efficiënt en effectief gebruik van communicatie, informatie en technologie door de veiligheidspartners.

De operationele doelstelling 25.1 richt zich op de versterking van de bestuurskracht van decentrale overheden en de randvoorwaarden die veiligheidspartners in staat stellen om hun werk efficiënt en

[8] Beleidsbegroting BZK 2007. Tweede Kamer, vergaderjaar 2006-2007, 30 800 hoofdstuk VII, nr. 2.
[9] "De Vrijblijvendheid Voorbij", Advies van de ACIR uitgebracht aan de minister van BZK, Maart 2005.
[10] Bestuurlijke rapportage rampenbestrijding en crisisbeheersing (BRRC 2007). Kenmerk 2007-0000438509.

effectief uit te kunnen oefenen. Operationele doelstelling 25.2 ondersteunt die versterking door specifiek de inzet van ICT.

2.4 Verantwoordelijkheid van de overheid

De verantwoordelijkheid van de overheid – in deze de minister van Veiligheid en Justitie – kent twee niveaus: een stelselverantwoordelijkheid (ook wel systeem of coördinerende verantwoordelijkheid genoemd) en een beleidsverantwoordelijkheid[11].

- Stelselverantwoordelijkheid betreft de verplichting rekenschap af te leggen voor het voldoende behartigen van een publieke taak.
  Zoals aangegeven in de beleidsbegroting 2012 strekt de stelsel- en coördinerende verantwoordelijkheid van de Minister van Veiligheid en Justitie zich uit tot het bestuurlijk bestel in zake veiligheid[12]. De minister is belast met het ontwikkelen van visie, beleid en samenwerkingsvormen op het terrein van de bestuurlijke aanpak van onveiligheid en criminaliteit. Inspanningen zijn erop gericht het lokaal bestuur zo effectief en efficiënt mogelijk in staat te stellen de lokale veiligheid te vergroten. De coördinerende verantwoordelijkheid wordt ingevuld samen met het lokale bestuur, onder andere via structurele overleggen met de G4, G32 en de Vereniging van Nederlandse Gemeenten (Veiligheidsregio's en veiligheidsberaad);
- Beleidsverantwoordelijkheid betreft een directe (politieke) verantwoordelijkheid.
  De Minister van Veiligheid en Justitie heeft een beleidsverantwoordelijkheid met betrekking tot lokale veiligheidsdossiers. Meer concreet gaat het daarbij om: het handhaven van de openbare orde en veiligheid, het vergroten van de leefbaarheid, het bestuurlijke voorkomen en afbreken van de verbinding van boven- en onderwereld. Tevens is hij direct verantwoordelijk voor een aantal systemen die als basisvoorziening dienen binnen het veiligheidsdomein[13].

---

[11] S. E. Zijlstra; "Bestuurlijk organisatierecht", Kluwer 2009, ISBN: 9789013067712.

[12] Tweede kamer, vergaderjaar 2011-2012, 33 000 VI, nr.2.

[13] Directie Nationale Veiligheid, brief aan de Tweede Kamer met kenmerk 312140 d.d. 12 december 2012.

3 De beleidsinstrumenten en realisatie

3.1 Inleiding

In dit hoofdstuk staat beschreven in welke mate de instrumenten die tot artikel 25.2 gerekend worden zijn gerealiseerd. Hierbij zijn die instrumenten geclusterd naar de indeling zoals die gehanteerd is in de begroting van het ministerie van Veiligheid en Justitie voor 2012. Bij deze beschrijving is ook ingegaan op de voor dit beleidsartikel relevante instrumenten die in de begrotingen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties voor 2007 t/m 2009 onder artikelen 4.2 en 4.3 stonden opgenomen.

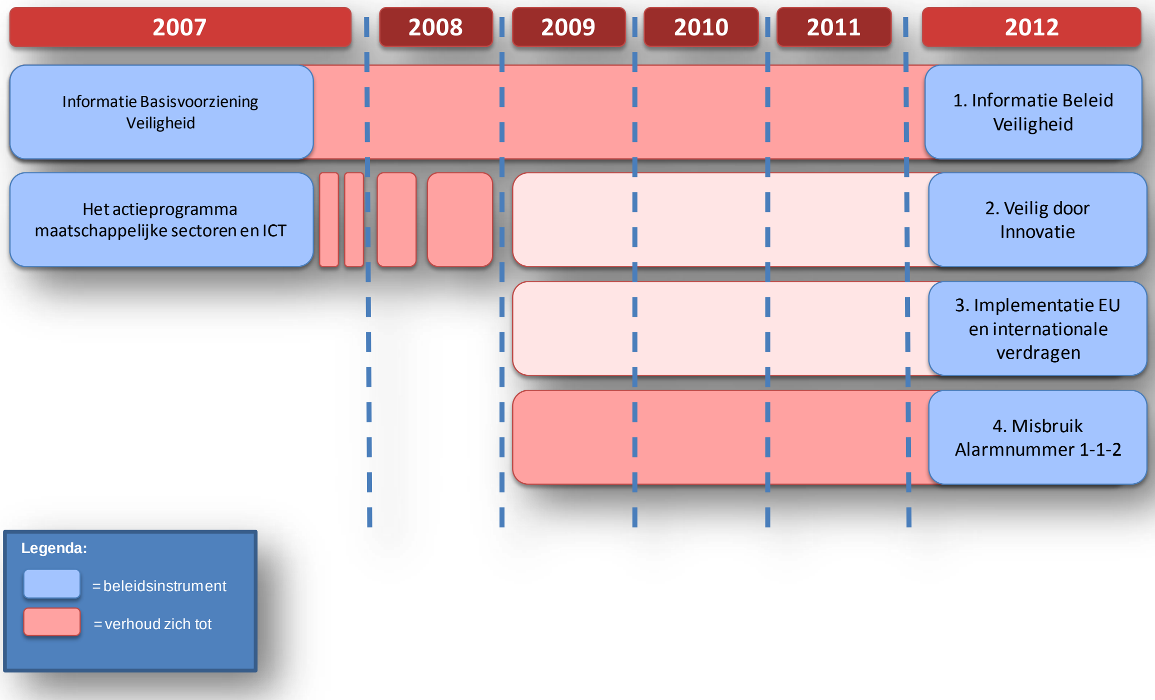
3.2 De ontologie van operationele doelstelling 25.2

De scope van deze beleidsdoorlichting wordt bepaald door de beleidsinstrumenten behorende bij de operationele doelstelling 25.2 van de beleidsbegroting van met ministerie van Veiligheid en Justitie in 2012. Binnen deze operationele doelstelling zijn de volgende vier beleidsinstrumenten gedefinieerd:

1. Informatie Beleid Veiligheid (IBV);
2. Veilig door Innovatie;
3. Implementatie van Europese en internationale verdragen;
4. Misbruik Alarmnummer 1-1-2.

De beleidsdoorlichting richt zich qua tijdspanne op de periode 2007 – 2012. Dit roept de vraag op hoe de bovengenoemde beleidsinstrumenten uit 2012 zich verhouden tot de beleidsinstrumenten in 2007. Onderstaande figuur geeft een vereenvoudigd beeld van de verhouding en daarmee van de scope van deze beleidsdoorlichting.

In bijlage E is een uitgebreide toelichting gegeven op de verhouding van artikel 25.2 (2012) tot artikelen 4.2 en 4.3 (2007) alsmede de ontwikkeling in tussenliggende jaren.



Instrument 1: Informatie Beleid Veiligheid

Met het instrument Informatie Beleid Veiligheid (IBV) faciliteert het Ministerie van Veiligheid en Justitie de politie, brandweer, GHOR en het lokaal bestuur bij het bevorderen van een samenhangende informatiehuishouding en goede communicatie binnen en tussen deze disciplines[14]. Dit beleidsinstrument relateert direct aan het (bijna gelijknamige) beleidsinstrument "Informatie Basisvoorziening Veiligheid (IBV)" uit 2007. Dit instrument is in de toenmalige begroting toegelicht als "De IBV is een virtuele structuur voor een gemeenschappelijke informatiehuishouding van de veiligheidpartners. Hiermee kan onder andere een uniforme bevraging van registers en een gemeenschappelijk beveiligingsbeleid worden bewerkstelligd". De scope van IBV 2007 valt daarmee binnen de scope IBV 2012. Centraal staat het scheppen van randvoorwaarden om de binnen en tussen de kolommen van het veiligheidsdomein tot goede informatie-uitwisseling te komen.

Naast deze meer randvoorwaardelijke aspecten vormt de vervanging van het Nationaal Noodnet (NN) door de Nood Communicatie Voorziening (NCV) een onderdeel van dit beleidsinstrument[15]. Het doel van

---

[14] Beleidsbegroting Ministerie van Veiligheid en Justitie, Tweede Kamer, vergaderjaar 2011-2012, 33 000 VI, nr. 2.

[15] Het NCV is benoemd binnen het beleidsinstrument IBV in 2012. In 2007 is het niet specifiek vermeld. Doordat in deze periode de verantwoordelijkheid voor het Noodnet (alsmede de vervanging ervan) overging van het ministerie van Economische Zaken naar het ministerie van BZK DGV (nu VenJ) én dit systeem past in het rijtje van landelijke informatievoorzieningen (naast C2000, GMS en LCMS) wordt dit meegenomen binnen de scope van de beleidsdoorlichting.

deze vervanging is het realiseren van een betrouwbaar “last resort” crisiscommunicatieplatform voor het Openbaar Bestuur en vitale sectoren dat primair voor spraakcommunicatie is ingericht maar op termijn mogelijkheden biedt om andere vormen van communicatie, zoals data en video, te ondersteunen[16]. Voor dit beleidsinstrument zijn geen prestatie-indicatoren opgenomen.

Instrument 2: Veilig door Innovatie

In de beleidsbegroting 2012 is het beleidsinstrument ‘Veilig door Innovatie’ opgenomen onder de operationele doelstelling 25.2. In de periode 2007 tot 2012 kende dit beleidsinstrument een voorloper in de vorm van het actieprogramma Maatschappij & ICT (M&ICT).

- Het actieprogramma M&ICT kende een doorlooptijd van 2006 tot en met 2009 en is als beleidsinstrument vermeld in de beleidsbegroting 2007 voor het onderdeel ‘veiligheid’. BZK vormde één van de zes participerende departementen in het actieprogramma dat zich richtte op het doorbreken van knelpunten bij het opschalen van kleinschalige, succesvolle ICT-toepassingen en –diensten. De regie en budgetten voor dit actieprogramma lagen bij het ministerie van Economische Zaken, het programmabureau was ondergebracht bij het ICTU. Het uitgangspunt voor het nationale R&D programma is gerichte opbouw van kennis en stimulering van innovatie en technologische toepassingen voor het veiligheidsdomein. Alleen onderzoeken waar spelers uit de veiligheidsketen zelf om vragen worden opgenomen in het programma. Met deze aanpak sluit BZK aan bij de rijksbrede vraaggestuurde onderzoeksprogrammering op TNO en de grote technologische instituten (Wijffels[17]).

- Het beleidsinstrument (programma) Veilig door Innovatie beoogd nieuwe technologieën op te leveren die het presterend vermogen van de veiligheidspartners verhogen. Dit programma is in de beleidsbegroting van BZK 2009 voor het eerst vermeld en in de beleidsbegroting van VenJ 2010 als beleidsinstrument benoemd. Het departementale programma vormt onderdeel van het interdepartementale programma Maatschappelijke Innovatie Agenda Veiligheid (MIAV). Met het aantreden van het kabinet Balkenende IV werd dit nieuwe interdepartementale innovatieprogamma gestart. In het beleidsprogramma van het kabinet werd onder pijler 2 en pijler 5 gekeken naar mogelijkheden om wetenschap en technologie een bijdrage kunnen leveren aan het oplossen van maatschappelijke problemen. De behoeftestelling voor beide pijlers was daarbij afkomstig uit de Kennisarena Maatschappelijke Veiligheid[18]. Hieruit is de interdepartementale maatschappelijke innovatieagenda veiligheid voort gekomen. Uit vergelijking van de maatschappelijke behoeften zijn drie thema’s (programmalijnen / roadmaps) vastgesteld:
    1. Opereren in ketens en netwerken waarbij het concept Network Enabled Capabilities (NEC) centraal stond;

16 Strategiedocument Noodcommunicatie Voorziening, 2008.

17 Om de kloof tussen onderzoek en de toepassing van resultaten (innovatieparadox) te verkleinen adviseert de commissie Wijffels om onderzoek bij TNO en de grote technologische instituten (GTI’s) zoals het NLR meer vraaggestuurd te programmeren.

18 MIAV publicatie juni 2008.

2. Simulatie, training en opleiding waarbij het gaat om het creëren van simulatieomgevingen (serious gaming) voor training en opleiding in het veiligheidsdomein;
3. Fysieke bescherming waarbij wordt ingezet op de bescherming van hulpverleners in een publieke functie.

De regie op de totstandkoming en uitvoering van de MIAV ligt bij de interdepartementale programmadirectie Kennis en Innovatie (KenI) en de deelnemende partijen zijn geclusterd binnen de Kennisarena Maatschappelijke Veiligheid.

De doelstellingen van zowel het programma Veilig door Innovatie als het actieprogramma maatschappelijke sectoren & ICT zijn niet nader geoperationaliseerd in prestatie-indicatoren op het niveau van de beoogde effecten.

Instrument 3: Implementatie EU en internationale verdragen

Dit beleidsinstrument wordt voor het eerst vermeld in de beleidsbegroting 2009 met de volgende generieke beschrijving: “Implementatie van Europese besluiten en Intergouvernementele verdragen”. In 2012 is het instrument nader geduid in drie componenten: het Verdrag van Prüm, de vervanging van de nationale component van het Schengen Informatie Systeem (SIS II) en de aansluiting van het Europol Informatie Systeem (EIS) aan de Basis Voorziening Opsporing (BVO van de Nederlandse Politie.

- Het Verdrag van Prüm is op 27 mei 2005 ondertekend door het Koninkrijk van België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Franse Republiek, het Groothertogdom Luxemburg, de Republiek Oostenrijk en het Koninkrijk der Nederlanden. Het Verdrag is door het Nederlandse Parlement geratificeerd en met ingang van 20 mei 2008 van kracht. Hiermee is een volgende stap gezet op het terrein van de politiële samenwerking in een deel van Europa. De onderwerpen in het Verdrag hebben betrekking op geautomatiseerde toegang tot gegevensverzamelingen voor DNA, vingerafdrukken en eigenaarschap van motorvoertuigen maar ook de samenwerking op het gebied van politieoptreden, uitzetting van vreemdelingen en de inzet van gewapende begeleiders van vliegtuigen (Airmarshals). De Europese Raad van Ministers van Justitie en Binnenlandse Zaken heeft de inhoud van de bepalingen van het Prüm verdrag in juni 2008 geïntegreerd in het rechtskader van de volledige Europese Unie (Raadsbesluit)[19]. In de beleidsbegroting 2012 ligt het accent op de fasegewijze uitbreiding van het aantal lidstaten, waarmee Nederland digitaal vingerafdrukken kan uitwisselen, naar uiteindelijk 27 lidstaten in 2013.
- Het project SIS II richt zich op de vervanging van de nationale component van het Schengen Informatie Systeem. Dit systeem heeft ten doel de uitwisseling van opsporingsinformatie in Europees en internationaal verband mogelijk te maken. De afronding van het project is voorzien in 2013.

[19] MGT-324 Eindrapportage project Prüm-Vingerafdrukken (versie 1.0)

- De derde component van dit beleidsinstrument betreft de operationeel maken van de gegevensuitwisseling tussen het Europol Informatie Systeem (EIS) en de Basisvoorziening Opsporing van de Nederlandse Politie[20].

Instrument 4: Misbruik alarmnummer 1-1-2

Het terugdringen van het misbruik van alarmnummer 1-1-2 is voor het eerst gemeld in de begroting van 2010. Hierbij is de volgende omschrijving gebruikt: “In 2010 wordt de locatie-informatie mobiele nummers en het terugbrengen van het misbruik van 112 geoptimaliseerd door de inzet van een aantal technische voorzieningen (voice-bommen, sms-bommen en voice-respons voor SIM-kaartloze 112 oproepen)”.

In oktober 2006 heeft de minister van BZK[21] aan ISC, voorloper van de vtsPN, de opdracht verstrekt de 1-1-2 alarmcentrale van het Klpd in Driebergen te vervangen. Deze nieuwe centrale is in 2009 in gebruikgenomen en heeft geleid tot een extra aantal oproepen omdat verbindingen sneller tot stand kunnen worden gebracht. Iedere burger moet in geval van nood (gratis en) direct met 1-1-2 contact kunnen krijgen. Daartoe is het technisch mogelijk om ook zonder simkaart 1-1-2 te bellen (“simless calls”). Een groot aantal “oneigenlijke” oproepen zou de bereikbaarheid van de 1-1-2 centrale onnodig kunnen belasten, waardoor de afhandeling van “echte” noodhulp-oproepen in gevaar zou kunnen komen. In circa 65% van de vier miljoen oproepen gaat het om oneigenlijk gebruik van het alarmnummer 1-1-2.

Binnen het oneigenlijke gebruik kan onderscheid worden gemaakt naar bewust en onbewust oneigenlijk gebruik. Bewust oneigenlijk gebruik is slecht een klein percentage van het oneigenlijk gebruik. Het onbewust oneigenlijk gebruik bestaat voornamelijk uit de zogenaamde “broekzakbellers”. Het bewust oneigenlijk gebruik van 1-1-2 bestaat voor een groot deel uit simless calls. Van deze simless calls is in 99,9% van de gevallen geen sprake van een noodhulpoproep. In 2010 is daarom ingestemd met het voornemen om de simless calls op provider niveau niet meer door te zetten naar de 1-1-2 centrale.

3.3 Realisatie instrument: Informatiebeleid Veiligheid (IBV)

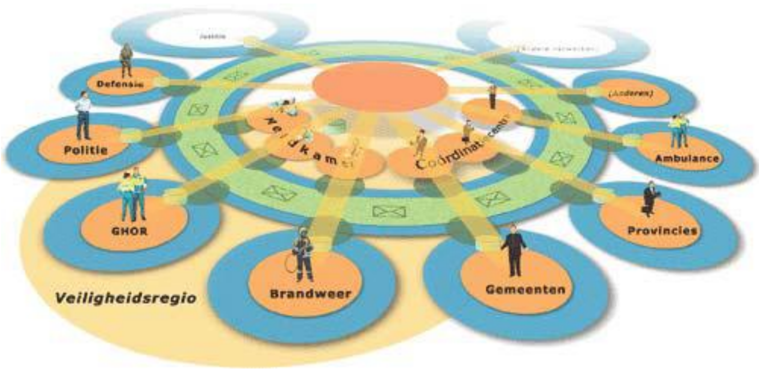
Het Informatiebeleid Veiligheid

Het IBV richt zich op het scheppen van randvoorwaarden om binnen en tussen de partners in het veiligheidsdomein te komen tot samenhangende en betere informatievoorziening. Het scheppen van deze randvoorwaarden is een complex proces. Het gebrek aan samenhang en informatie-uitwisseling is immers geen eenzijdig technologisch vraagstuk. Juist door de versnippering van verantwoordelijkheden en autonomie van verschillende partners in het veiligheidsdomein ontstond een gebrek aan eenduidige afspraken waaraan informatievoorziening voor de gehele veiligheidsketen aan zou moeten voldoen. Het IBV heeft door een overkoepelende visie te ontwikkelen op drie niveaus bijgedragen aan verbetering van de samenhangende informatievoorziening. Deze drie niveaus zijn weergegeven in het Galaxy model waarbij de oranje kleur bestuurlijke afspraken betreft; de groene kleur standaarden en architectuur betreft om verschillende soorten informatie te delen; en de blauwe kleur technische standaarden betreft. Het Galaxy model is onderstaand weergegeven:

---

[20] Beleidsbegroting Ministerie van Justitie, Tweede Kamer 2011-2012, 33 000 VI, nr.2.

[21] Brief BZK van 5 oktober 2006, kenmerk 2006-0000157354, met offerte ISC van 11 april 2006



In 2009 zijn richtinggevende principes ten aanzien van Organisatie & Bestuur, Juridisch, Financieel, Beheersmatig, Informatiekundig en Techniek uitgewerkt in een manifest[22]. Deze principes zijn in dialoog met de verschillende veiligheidspartners opgesteld en gebaseerd op bestaande kaders en architecturen die in verschillende domeinen al zijn ontwikkeld met als vertrekpunt de Nederlandse Overheid Referentie Architectuur (NORA). De principes zijn echter niet dwingend aan de partners in het veiligheidsdomein op te leggen (als gevolg van de eerder genoemde autonomie). Het IBV (Galaxy model) en de IBV principes zijn daarom in constante dialoog en afstemming met alle relevante partners tot stand gebracht. Het IBV is daarbij van invloed geweest en heeft waar mogelijk als uitgangspunt gediend bij een aantal belangrijke samenwerkingsprojecten binnen het veiligheidsdomein.

- *Afspraken in het project Informatie Architectuur Sector Veiligheid (IASV)*
  In 2008 is onder verantwoordelijkheid van de Raad voor Multidisciplinaire Informatievoorziening Veiligheid (Raad MIV) een portfolio-overzicht opgesteld van lopende trajecten/activiteiten voor de verbetering van de informatievoorziening binnen en tussen de verschillende veiligheidspartners. In de periode 2007-2009 is het project Informatie Architectuur Sector Veiligheid (IASV) uitgevoerd. Het doel van de IASV was het realiseren van een eenduidig referentiekader voor de uitwisseling van informatie bij rampen en crises. Het IBV vormde hierbij het uitgangspunt. Hiervoor heeft het IASV-project 127 multidisciplinaire informatieproducten benoemd en met kwaliteitskenmerken uitgewerkt. De term 'multidisciplinair' betekent dat het informatieproduct tussen meerdere partners (brandweer, gemeente, politie en GHOR) gedeeld wordt. Daarnaast heeft het project IASV samen met de veiligheidspartners twaalf multidisciplinaire informatieproducten in detail uitgewerkt. Deze informatieproducten vormen de kern van het multidisciplinaire gedeelde beeld;
  - Incident informatie (incl. grip status)
  - (Beeld van het) effect
  - Getroffeneninformatie
  - Situatie/voortgang rapportage (Sitrap)
  - Probleemvelden (afwijkingen, knelpunten, issues etc.)
  - Ingezet personeel of eenheid
  - Voorlichting
  - Besluiten
  - Actiepunten (incl. instructies)

[22] Manifest Principes Informatiebeleid veiligheid, 2009

- Adviezen
- Operationele locaties (een 40 tal locaties waar inzet kan plaatsvinden incl. geosymbolen)
- Ad hoc informatie of mededelingen

- *Project Netcentrisch Werken*
  Het project Netcentrisch Werken ondersteunde de veiligheidsregio's, het NCC en het LOCC bij het invullen van het aspect informatievoorziening van het Besluit veiligheidsregio's. Daarbij gaat het vooral om het implementeren van een werkwijze die het mogelijk maakte om binnen de hoofdstructuur van de crisisorganisatie bij opschalingsituaties snel te komen tot een eenduidig en over verschillende lagen gedeeld totaalbeeld van de situatie. Aanleiding voor dit project was het RADAR-onderzoek van de Inspectie OOV (2009) waarin werd geconstateerd dat het overgrote deel van de veiligheidsregio's tekort schoot op het gebied van informatiemanagement[23]. In de jaren daarvoor werd overigens ook al geëxperimenteerd met netcentrisch werken. Zo werd de werkwijze als 'proof-of-concept' toegepast in de landelijke crisisoefening 'Voyager' in oktober 2007. Volgens de evaluatie, uitgevoerd door TNO, leverde de netcentrische werkwijze een versnelling op in de beeldvorming, met meer tijd voor oordeels- en besluitvorming[24]. Hierdoor waren alle betrokkenen beter in staat hun eigen verantwoordelijkheden en bevoegdheden in te vullen. Bovendien was de betrouwbaarheid van de informatie hoger en bleven tijdrovende verificatieslagen achterwege. Deze evaluatie heeft geleid tot het besluit om binnen alle veiligheidsregio's het netcentrisch werken te implementeren en te ondersteunen met een Landelijk Crisismanagement Systeem (LCMS). Het Veiligheidsberaad besloot in 2009 tot de uitvoering van het landelijk project Netcentrisch Werken. Momenteel is deze werkwijze ondersteund door het LCMS, in bijna all veiligheidsregio's, het LOCC en het NCC geïmplementeerd[25]. Daarnaast is het netcentrische gedachtegoed is door het project in samenwerking met TNO vastgelegd in het 'Referentiekader Netcentrische Crisisbeheersing'. Dit referentiekader is eind 2012 door het Veiligheidsberaad vastgesteld. Voorafgaand aan de bestuurlijke vaststelling is het Referentiekader besproken en goedgekeurd in het Landelijk Projectleiders Overleg, de Stuurgroep Netcentrisch Werken, het Disciplineoverleg Informatievoorziening, de Programmaraad Informatiemanagement, de Programmaraad Crisisbeheersing en Rampenbestrijding, de GHOR, het Portefeuilleoverleg Crisisbeheersing, het Portefeuilleoverleg Informatievoorziening en de Bestuurlijke Adviescommissie Informatievoorziening[26].

- *Informatiebeleidsplannen per kolom*
  Het IBV gedachtegoed heeft bijgedragen aan de vorming van informatiebeleidsplannen van de GHOR, de brandweer en de politie. Het herziene landelijk brandweer informatiebeleidsplan "In helder perspectief" is bestuurlijk geaccordeerd door de Raad van Regionaal Commandanten van de NVBR, de Raad MIV en de Bestuurscommissie Brandweer van het Veiligheidsberaad[27]. Een landelijke vraagorganisatie die de behoefte aan informatievoorziening bundelt en per thema programma's van eisen opstelt, is in 2009 opgezet. Er is invulling gegeven aan het digitale bereikbaarheidsconcept door een proof-of-concept van de bereikbaarheidskaart uit te laten uitvoeren. Ook GHOR Nederland is in

---

23 Nieuwsbrief Inspectie Openbare Orde en Veiligheid, Jaargang 8, nummer 1 (juni 2009)
24 Managementsamenvatting Referentiekader Netcentrische crisisbeheersing, september 2012 – versie 1.0.2
25 Managementsamenvatting Referentiekader Netcentrische crisisbeheersing, september 2012 – versie 1.0.2
26 Veiligheidsberaad stelt Referentiekader netcentrische Crisisbeheersing vast. Crisisplein.nl.
27 In_helder_pespectief_rev2009_juni_wijzigingen.doc. (29 juni 2009)

2009 gestart met een landelijk beleidsplan informatievoorziening. Dit landelijk beleidsplan informatievoorziening is in 2010 door het Veiligheidsberaad vastgesteld. Binnen de politiekolom hebben zich de afgelopen jaren ingrijpende ontwikkelingen voorgedaan. De Inspectie Openbare Orde en Veiligheid (OOV) heeft eind 2008 gerapporteerd over de realisatie van de afspraken met betrekking tot het tot stand brengen van een uniforme informatiehuishouding bij de politie. In het daaropvolgende kabinetsstandpunt "Samenwerkingsafspraken en Politiewet" (Kamerstukken II 2008-2009, 29 628, nr. 110) is aangegeven welke verbeteringen benodigd waren en dat in 2010 een nieuwe evaluatie door de IOOV zou plaatsvinden. In de tussenliggende periode is sprake geweest van een ernstige uitval van de ICT-systemen in Noord-Oost-Nederland. De Inspectie OOV trekt op basis van haar onderzoek in 2010 de volgende conclusies: "*De beoogde betere samenwerking tussen de korpsen is onvoldoende gerealiseerd. De korpsen wisselen meer informatie uit dan voorheen maar nog onvoldoende en onvolledig. Van echt informatie delen is nog maar beperkt sprake. De drie basis ICT-systemen worden niet op uniforme wijze gebruikt en functioneren ook niet optimaal. Er zijn grote risico's genomen bij de implementatie van de basisvoorzieningen waardoor de betrouwbaarheid en continuïteit van de informatievoorziening op het spel stonden. Het gemeenschappelijk functioneren van de Nederlandse politie is in dit opzicht niet verbeterd*"[28]. Deze conclusies hebben bijgedragen tot het opstellen van het aanvalsprogramma Informatievoorziening Politie 2011-2014. Daarnaast is, met de vorming van de Nationale Politie, de governance verbeterd en doorzettingsmacht gecreëerd.

Vervanging Nationaal Noodnet

De Telecommunicatiewet is aangepast om een opvolger van het Nationaal Noodnet (NN) te kunnen realiseren. De wet schreef namelijk voor dat KPN de verplichting had een communicatievoorziening in stand te houden welke in te zetten was in noodgevallen wanneer alle andere communicatie onmogelijk was (noodnet). Deze wet zou een aanbesteding in de weg staan aangezien KPN op dat moment een marktpartij was geworden en er dus concurrentie mogelijk was. Er heeft in 2008 een niet-openbare aanbesteding plaats gevonden waarna in december 2009 KPN de formele opdracht kreeg. (Bron: Respondent)

De uitrol van de opvolger van het Nationaal Noodnet (NN), de Noodcommunicatievoorziening (NCV), is gestart in het najaar van 2010. Zoals aan de Kamer is gemeld in de 3e brief Nationale Veiligheid (TK 2009-2010 30821, nr. 10) is de NCV met ingang van 1 mei 2011 operationeel en bruikbaar voor de gemigreerde gebruikers. Gedurende de migratie van gebruikers van NN naar NCV blijft ook het oude NN in functie. Verwacht werd dat de meeste gebruikers van het NN na het in gebruik nemen van NCV op korte termijn opdracht zouden geven voor migratie naar de NCV. In de praktijk blijkt de migratie meer tijd te kosten. Een groot aantal gebruikers benut de beëindiging van de overeenkomst met het NN om een zorgvuldige heroverweging te maken en de vraag te beantwoorden welke partijen moeten worden aangesloten. Daarnaast zijn voorgenomen herindelingen van gemeenten en plannen ten aanzien van samenvoegen van meldkamers aanleiding om geen overhaaste beslissing te nemen. Ook waren er veel vragen over, met name de extra functionaliteiten die in de NCV beschikbaar zijn. Al deze factoren zijn redenen waarom de migratie trager op gang gekomen is. De noodcommunicatievoorziening is echter niet in gevaar gekomen omdat het NN nog functioneert. Er is sinds de ingebruikneming van de NCV geen sprake van beschikbaarheidverlies van functionaliteit van de noodcommunicatie[29].

---

[28] Onderzoek Samenwerkingsafspraken Politie 2008 – stand van zaken 2010. Inspectie Openbare Orde en Veiligheid

[29] *Bron: beantwoording Kamervragen - Kenmerk: 2012-0000048892*

3.4 Realisatie instrument: Veilig door innovatie

Zoals aangegeven in paragraaf 3.2 is voor dit beleidsinstrument onderscheid gemaakt in twee programma's die in de periode 2007 tot 2012 een gedeelde doelstelling hadden: het vergroten van veiligheid door het stimuleren van innovatie en het ontsluiten van innovatieve oplossingen. Innovatie staat centraal. Daarnaast kenmerken de twee programma's zich doordat de stimulans of ontsluiting wordt gerealiseerd door toekenning van financiële middelen (subsidie).

1. *Programma Maatschappelijke Sectoren en ICT (M&ICT)*
   Het rijksbrede programma M&ICT is specifiek voor opschaling van ICT-projecten in het leven geroepen. In vier jaar tijd is vanuit M&ICT een scala aan ICT-projecten financieel ondersteund. Belangrijke doelstelling daarbij was de vraagarticulatie door partners uit de veiligheidsketen zelf. In de jaren 2007 tot en met 2009 zijn de partners in de veiligheidsketen van begin tot einde bij de onderzoeken betrokken. De eerste stap in het onderzoeksproces, het formuleren van onderzoeksbehoeften, gebeurt in de Arena Maatschappelijke Veiligheid. Een arena is een vorm van samenwerken waarbij innovatiebehoeften vanuit verschillende invalshoeken worden aangedragen en op elkaar afgestemd. Aangezien Maatschappelijke veiligheid een breed gebied beslaat, was de arena opgedeeld in acht thematische subarena's:
   - Terrorisme en radicalisering;
   - Dreigings-,risicoherkenning en analyse;
   - Veel voorkomende criminaliteit en overlast;
   - Veiligheid van netwerksystemen;
   - Versterking van opsporing en handhaving;
   - Geïntegreerde systemen;
   - Uitrusting en materieel;
   - Opleiden en oefenen.

   De subarena's bestonden uit vertegenwoordigers van eindgebruikers, kennisinstellingen en bedrijven die opereren in het domein van maatschappelijke veiligheid. De inventarisatie van de onderzoeksbehoeften vond plaats in de verschillende subarena's. De beoordeling van de onderzoeksbehoeften vond plaats binnen BZK. In totaal werden twaalf prijsvragen met wisselende thema's georganiseerd, met als resultaat dat bijna 400 projectvoorstellen (rijksbreed) werden ingediend. Daarvan zijn 63 ICT-opschalingsprojecten (rijksbreed) gehonoreerd waarvan de volgende acht in de domein veiligheid[30]:
   - Beter voorbereid op incidenten en rampen;
   - Digitale Bereikbaarheidskaart;
   - Innovatie Beveiligings- en Alarmeringsketen;
   - Landelijke Databank Risicotaxatie tbs;
   - Multi-VIT;
   - Portfolio Multidisciplinaire Informatievoorziening Veiligheid;
   - Samen voorbereid veilig;
   - Slimmer veilig.

   Alle projecten zijn door middel van een standaard evaluatieformat geëvalueerd door het programmabureau M&ICT binnen het ICTU. Daarbij zijn geen financiële onvolkomenheden

[30] Boek "Maatschappelijke Sectoren en ICT, Uitgave ICTU, 2009.

vastgesteld. De regeling hield eind 2009 op. In een evaluatie van het gehele programma concludeert TNO het volgende[31]: *Het Actieprogramma Maatschappelijke Sectoren & ICT heeft op directe en op indirecte wijze een bijdrage geleverd aan het doorbreken van belemmeringen in de opschaling van maatschappelijk relevante ICT-toepassingen: op directe wijze door materiële en immateriële ondersteuning van in totaal 63 projecten; op indirecte wijze doordat afgewezen consortia soms door zijn gegaan en voor eigen rekening opschaling hebben gerealiseerd. Bij de gehonoreerde projecten zijn verschillende interessante toepassingen gerealiseerd die succesvol zijn geweest in het doorbreken van belemmeringen voor opschaling en die een aantoonbare bijdrage leveren aan het oplossen van een maatschappelijk vraagstuk. Bij de afgewezen projectvoorstellen bestaat anekdotisch en incompleet bewijs voor de conclusie dat de gevormde consortia voor eigen rekening verder zijn gegaan. Conclusie: Het Actieprogramma heeft in grote lijnen voldaan aan zijn doelstellingen. Het heeft een duidelijke bijdrage geleverd aan het doorbreken van belemmeringen in het opschalen van maatschappelijk relevante ICT-toepassingen.*

Het actieprogramma zit in de periode 2010 – 2012 in een 'passieve fase', waarin het de voortgang van de nog lopende projecten monitort. Daarnaast is er aandacht voor het overdragen en borgen van de kennis en de ervaring die in de projecten is opgedaan.

2. *Project Veilig door Innovatie / Maatschappelijke Innovatie Agenda Veiligheid (MIAV)*
   Het project Veilig door Innovatie zoals opgenomen binnen de beleidsbegrotingen van het ministerie van VenJ (2010, 2011 en 2012) is onderdeel van het interdepartementale programma MIAV. De MIAV is in 2008 voorbereid en van start gegaan. Daarbij zijn drie programma's opgezet, die tegelijk de drie gemeenschappelijke interdepartementale gebieden vormen: Opereren in ketens en netwerken; Simulatie en training en Fysieke bescherming. Deze programmalijnen zijn tot stand gekomen op basis van inventarisatie van trends, taken, behoeften en technologiegebieden van de deelnemende ministeries Defensie, Binnenlandse Zaken en Koninkrijksrelaties en Justitie. Voor elk programma zijn zogenaamde roadmaps opgesteld waarin de inhoudelijke programmering is opgenomen. De programma's zijn ondergebracht in drie werkgroepen waarbij SenterNovem ondersteuning verzorgde. Het doel van de MIAV is het daadwerkelijk oplossen van maatschappelijke problemen en tegelijkertijd, door in een zo vroeg mogelijk stadium bedrijfsleven en kennisinstellingen te betrekken, innovaties op gang te brengen. In het startdocument is daarbij de aanbeveling gedaan de relatie met bestaande initiatieven en programma's te versterken: "*De overheid investeert al een aantal jaren flink in publiek-private technologie-ontwikkeling … Het verdient aanbeveling om de initiatieven en programma's die raakvlakken hebben met de zeven sterke Nederlandse clusters, te betrekken bij het ontwikkelen van de maatschappelijke innovatieagenda veiligheid*"[32]. Dit citaat signaleert de veelheid aan initiatieven op het gebied van innovatie en de onderlinge verwevenheid. Hierdoor én de nadruk op maatschappelijke verbondenheid is de MIAV ondergebracht binnen de interdepartementale directie Kennis en Innovatie en vormt onderdeel van het kabinetsproject Nederland Ondernemend Innovatieland (NOI). De MIAV valt qua uitvoering onder de subsidieregeling 'innoveren' van het ministerie van Economische Zaken[33]. Onder deze regeling kunnen projecten worden ingediend ter subsidiëring Deze projecten dienen te passen binnen de doelstelling van de MIAV en werden

---

[31] TNO rapport 35236 "Opschaling van relevante maatschappelijke ICT toepassingen, lessen uit de praktijk". 23-2-2010.

[32] MIAV publicatie juni 2008

[33] Staatcourant 2009 nr. 11299, 27 juli 2009

inhoudelijk beoordeeld door een Adviescommissie op basis van vooraf vastgelegde criteria. In de navolgende jaarverslagen van het ministerie van BZK zijn de volgende verantwoordingsstatements inzake de uitvoering van het project Veilig door Innovatie opgenomen. In 2009 is door MinDEF, MinJUS en MinBZK een Maatschappelijke Innovatie Agenda Veiligheid uitgewerkt aan de hand van drie gemeenschappelijke thema's: optreden in ketens en netwerken, opleiden en trainen met behulp van geavanceerde simulatie en fysieke bescherming. Voor deze thema's zijn roadmaps gemaakt [bron: Jaarverslag BZK, 2009]. In 2010 zijn de volgende vier producten opgeleverd: een optimalisatie in het proces van de arrestantenafhandeling (ARAF), een volledig zelfstandig instrument voor het zoeken naar kinderporno op wensites (Webcrawler), modus-operandi onderzoek als kennisbasis ter voorkoming van woninginbraken en het cobra blussysteem waarmee op een veilige manier van buitenaf een blusaanval kan worden ingezet. Er zijn verschillende onderzoeken uitgevoerd in het kader terrorismebestrijding (herkennen afwijkend gedrag met camerabeelden) en ten aanzien van chemische/nucleaire incidenten (bijv. ontsmettingsprocedures en bestrijdingstechnieken) [bron: Jaarverslag BZK, 2010]. Het project heeft in 2011 de volgende producten opgeleverd: procesbesturingssystemen Hermes, Castor en Midas die bijdragen aan veiligheid netwerksystemen vitale sectoren, virtuele rook & vuur module als serious game om brandbestrijding te oefenen. Daarnaast is aansluiting gevonden bij het Topsectorenbeleid en zijn de Nederlandse belangen behartigt binnen het 7de Kaderprogramma van de EU[34].

In de subsidieregeling[35] is een controleprotocol opgenomen aangaande het geven van aanwijzingen over de reikwijdte en intensiteit van de accountantscontrole van EZ subsidies. Elk project uitgevoerd binnen MIAV diende een accountantsverklaring af te geven die beschikbaar werd gesteld aan de departementale Auditdienst. Daarmee is rechtmatigheid van de besteding van financiële middelen door voornoemde projecten geborgd. Uit de interviewronde en beschikbare gestelde documentatie kan niet worden vastgesteld dat evaluaties hebben plaatsgevonden inzake de doelmatigheid of doeltreffendheid van de MIAV projecten.

[34] Jaarverslag en slotwet Ministerie van Veiligheid en Justitie 33 240 VI, aangeboden 16 mei 2012
[35] Staatcourant 2009 nr. 11299, 27 juli 2009

3.5 Realisatie instrument: Europese en internationale verdragen

Bij de beschrijving van de realisatie van dit beleidsinstrument is onderscheid gemaakt naar de drie componenten (zie beschrijving in paragraaf 3.2).

- *Het verdrag van Prüm.*
  Op 25 januari 2013 is de eindrapportage project Prüm-Vingerafdrukken opgeleverd aan de stuurgroep inclusief een evaluatie en aanbevelingen voor het vervolg[36]. Dit project is in 2009 gestart. In het toenmalige Project Initiatie Document is de doelstelling als volgt geformuleerd: "*het bestuurlijk, procesmatig, organisatorisch en technisch inrichten van de geautomatiseerde uitwisseling van dactyloscoptische gegevens tussen Nederland en de aangesloten Prüm-landen waardoor voldaan wordt aan het Raadsbesluit Prüm (Europese wet)*[37]". Daarbij was de eis dat de geautomatiseerde uitwisseling van vingerafdrukkengegevens conform Raadsbesluit uiterlijk 26 augustus 2011 operationeel diende te zijn. Zoals in het eindrapport wordt geconcludeerd is de beoogde doelstelling van het project (met vertraging) behaald. Het project is opgeleverd in januari 2013. De gerealiseerde doorlooptijd is daardoor 29 maanden, een vertraging van 10 maanden ten opzichte van het initiële PID. Als belangrijkste redenen voor deze vertraging zijn genoemd[38]:
  - Besluitvorming over beleggen processen vertraagd (2010);
  - Projectleider vtsPN later aan boord dan gepland (2010);
  - Doorlooptijd EU-evaluatie langer dan begroot (2011);
  - Formele toewijziging van de benodigde extra (8) formatieplaatsen en de werving en selectie daarvan (2010/2011)
  - Verlaagde beschikbaarheid testsysteem en personeel door koppeling IWPI-HAVANK (2011);
  - Beperkte capaciteit interne organisatie IPOL voor uitwerken werkinstructies (2011);
  - Inrichten portaal vtsPN duurde langer dan gepland (2011);
  - Procedure inspoelen software op productiesysteem duurde langer dan gepland (2011);
  - Inconsistentie tussen test -, acceptatie en productiesysteem waardoor het testen en invoeren van nieuwe releases niet lukte. Herstelperiode voor functioneel beheer en vtsPN (2011-2012)
  - Afbouwen / vertrek van enkele projectmedewerkers (2012).

- *Vervanging van de nationale component van het Schengen Informatie Systeem (SIS II)*
  Voor de uitwisseling van opsporingsinformatie in Europees en internationaal verband wordt sinds 1995 gebruik gemaakt het Schengen Informatie Systeem (SIS). SIS bestaat uit een centraal systeem waarop de nationale SIS systemen aangesloten zijn. Dit systeem is echter technische verouderd en bevat geen mogelijkheid (meer) tot het uitbreiden van lidstaten. Daarom wordt er vanaf 2007 gewerkt aan de totstandkoming van SIS-II. De uiteindelijke implementatie van SIS-II is vertraagt vanwege aanpassingen in de technische specificaties. Deze aanpassingen hebben niet alleen de vertraagde realisatie tot gevolg, maar hebben ook een kostenverhogend effect. Dit omdat het nationale projectteam langer operationeel moet blijven en omdat het NSIS-II (de nationale component) aangepast moet worden aan de technische specificaties van SIS-II. Zowel de vertragingen

---

[36] MGT-324 Eindrapportage project Prüm-Vingerafdrukken (versie 1.0)

[37] Het verdrag van Prüm is omgezet in raadsbesluiten 2008/615/JBZ en 2008/616/KBZ.

[38] MGT-324 Eindrapportage project Prüm-Vingerafdrukken (versie 1.0)

als de kostenverhogingen die daaruit resulteerden (van 8,6 miljoen euro naar uiteindelijk 22,8 miljoen euro) zijn gemeld in het AO JBZ-raad. Oplevering is nu voorzien in 2013.

- *Operationeel maken van de gegevensuitwisseling tussen het Europol Informatie Systeem (EIS) en de Basisvoorziening Opsporing van de Nederlandse Politie*
  Door Europol is het Europol Informatie Systeem (EIS) ontwikkeld waarmee informatie over zware georganiseerde criminaliteit tussen de EU lidstaten en enkele derde landen uitgewisseld kan worden. Met dit systeem kan door een land worden vastgesteld of personen of objecten in opsporingsonderzoeken in andere deelnemende landen voorkomen. Indien dit het geval is kan bilateraal meer informatie worden uitgewisseld (dus niet via EIS) en eventueel ook worden samengewerkt. Voor Nederland verloopt de koppeling van EIS via een nationale adapter met de Basisvoorziening Opsporing (BVO). Op dit moment zijn alleen de KLPD en de (voorheen) korpsen van Flevoland, Gooi en Vechtstreek en Utrecht aangesloten. De verdere ontwikkeling is opgeschort tot het gereed komen van Summ-IT als opvolger van BVO voor de Nationale Politie.

De doelstellingen van het instrument “Implementatie EU en internationale verdragen” zijn niet geoperationaliseerd in prestatie-indicatoren. Op het afsluitende ‘Prüm congres’ over vingerafdrukken zijn meerdere voorbeelden gepresenteerd waarbij is getoond dat de implementatie van dit verdrag daadwerkelijk heeft bijgedragen aan het oplossen van strafbare feiten (casus witwassen in relatie tot Litouwen en casus persoonsidentificatie)[39]. Ook Europol laat regelmatig zien dat de via EIS opgebouwde informatiepositie heeft bijgedragen aan het beheersen van de zware georganiseerde criminaliteit[40].

3.6 Realisatie instrument: Misbruik alarmnummer 1-1-2

Een breed pakket aan maatregelen is inmiddels ingezet door de landelijke eenheid van de politie (voormalig Klpd) waaronder het gebruik van de “voice-bom” en de ”sms-bom” om de bellers te wijzen op het feit dat zij bewust dan wel onbewust contact hebben gelegd met 1-1-2. De voice-bom betekent dat er een gesproken bericht naar de betreffende telefoon verstuurd wordt, die afgeluisterd moet worden door de gebruiker van de telefoon. Het bericht kan niet worden gewist zonder te beluisteren. Een sms-bom is hiermee vergelijkbaar, alleen bevat deze een geschreven bericht. Op deze wijze wordt het oneigenlijke gebruik bestreden. Om het bewust misbruik terug te dringen heeft in 2010 een media campagne plaatsgevonden om de doelgroep hiervan bewust te maken[41] .

Daarnaast wordt er gewerkt aan het uitsluiten van simless calls op provider niveau om het oneigenlijke gebruik drastisch terug te dringen. In tegenstelling tot eerdere afspraken heeft het ministerie van Economische Zaken aangegeven dit niet via de Telecomwet geregeld kan worden. Sindsdien wordt er gewerkt aan een alternatieve oplossing. Met de telecomproviders wordt gewerkt aan de totstandkoming van een convenant waarin afgesproken moet worden op welke technische wijze de simless calls niet meer bij de landelijke 1-1-2 centrale binnenkomen. Gedurende dit proces trok een van de drie grote providers zich terug uit de onderhandelingen en wilde uitsluitend verder op basis van een commercieel voorstel. Uiteindelijk is er door het ministerie van VenJ gevraagd onder welke financiële voorwaarden deze drie

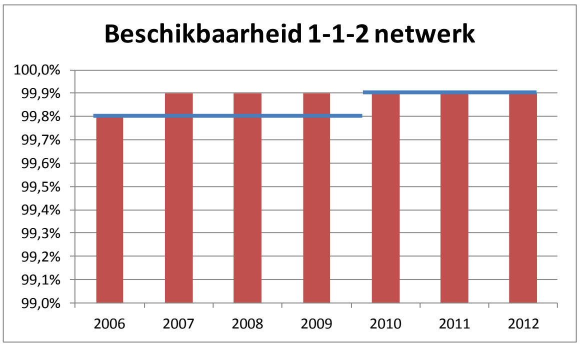
[39] Symposium Prüm Vingerafdrukken – de Poort naar Europa 4 december 2012.

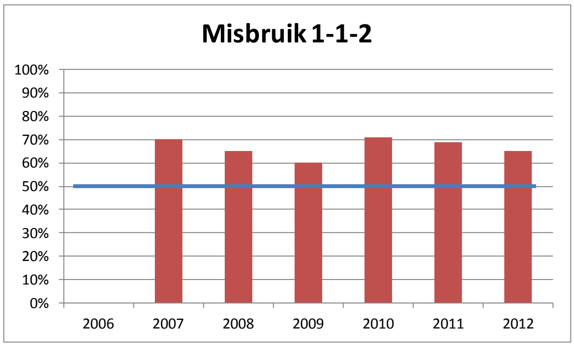
[40] EDOC-#647657-v1-SIENA_monthly_report_December_2012.doc d.d. 2 januari 2013.

[41] Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2010, Tweede Kamer, vergaderjaar 2010–2011, 32 710 VII, nr. 1

providers de ongewenste gesprekken wilden blokkeren. Twee van de drie (grote) providers deden een vergelijkbare aanbieding, echter de derde partij was substantieel duurder. Volgens de respondent probeert het ministerie de hierdoor ontstane patstelling nu te doorbreken door een diepgaande analyse te maken van de simless calls en van daaruit met de providers in gesprek te treden. Hiertoe zijn in 2012/2013 metingen verricht die duidelijk moeten maken hoe de stromen van simless calls verlopen en hoe deze zijn uit te sluiten van doorgeleiding naar de landelijke alarmcentrale.

Binnen artikel 25.2 is uitsluitend voor het instrument “tegengaan misbruik alarmnummer 1-1-2” indicatoren ontwikkeld en gevuld:





Bron: Jaarveslag BZK 2011, VenJ 2012.

De norm voor de beschikbaarheid van het 1-1-2 netwerk is 99,9%. Deze norm wordt vanaf 2007 reeds gerealiseerd.

De tweede indicator betreft het terugdringen van het aantal onterechte 1-1-2 telefoontjes. De norm voor het misbruik is bepaald op maximaal 50%. Na een daling van 70% in 2007 naar 60% in 2009 is dit percentage in 2010, o.a. als gevolg van een aanpassing in het netwerk van een provider, weer opgelopen tot boven het niveau van 2007 70,9% . In 2011 is de daling van het aandeel misbruik weer ingezet (68,8%) en in 2012 doorgezet naar 65%. De convenanten met de providers zouden de laatste zet moeten zijn om de komende jaren onder de 50% grens te komen[42].

3.7 Conclusies

Gesteld kan worden dat alle beleidsinstrumenten het efficiënt en effectief gebruik van communicatie, informatie en technologie hebben bevorderd. Echter, doordat de begrippen ‘*bevorderen’, ‘efficiënt’* en *‘effectief*’ niet nader zijn geoperationaliseerd in prestatie-indicatoren voor drie instrumenten is het niet vast te stellen in welke mate deze bevordering van ICT heeft plaatsgevonden. Op basis van de beschikbare documentatie en de interviews is voor deze instrumenten wel een plausibele relatie vast te

[42] Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2010, Tweede Kamer, vergaderjaar 2010–2011, 32 710 VII, nr. 1 en Jaarverslag en slotwet Ministerie van Veiligheid en Justitie 2011, Tweede Kamer, vergaderjaar 2011–2012, 33 240 VI, nr. 1

stellen tussen de uitvoering van de beleidsinstrumenten en een aantal resultaten in het veiligheidsdomein:

- De samenwerking tussen partners in het veiligheidsdomein is verbeterd door constante dialoog inzake bestuurlijke afspraken, architectuur en technische standaarden. Deze samenwerking komt tot uiting binnen en tussen de kolommen van het veiligheidsdomein (waaronder IASV, NEC, LCMS en de informatiebeleidsplannen per kolom).
- Het Nationaal Noodnet is vervangen door de Nood Communicatie Voorziening. Met dit crisiscommunicatieplatform is de communicatie tussen de aangesloten vitale sectoren ten tijde van grootschalige ICT uitval geborgd.
- De innovatieprogramma's hebben geleid tot een veelheid aan nieuwe technologieën (of toepassingen daarvan) in het veiligheidsdomein. Door de criteria en het beoordelingsproces voor de subsidietoekenning is aansluiting bij het overkoepelende doel (bevordering van nieuwe technologieën die breed toepasbaar zijn) geborgd.
- De implementatie van het verdrag van Prüm is, met enige vertraging, in januari 2013 gerealiseerd. Met dit verdrag is een geautomatiseerde uitwisseling van vingerafdrukgegevens tussen lidstaten mogelijk.
- Via een nationale adapter is het Europol Informatie Systeem (EIS) gekoppeld aan de BVO (Basisvoorziening Opsporing) van de KLPD en de (voorheen) politiekorpsen in de regio Midden-Nederland (Flevoland, Gooi en Vechtstreek en Utrecht). De verdere ontwikkeling is opgeschort tot het gereed komen van Summ-IT als opvolger van BVO binnen de Nationale Politie.

Binnen het beleidsdoelstelling 25.2 zijn alleen voor het beleidsinstrument 'misbruik alarmnummer 1-1-2' prestatie-indicatoren geformuleerd. Hierdoor is het mogelijk om jaarlijks de realisatie voor dit instrument te meten tegen de afgesproken norm.

- De inzet van voice-bommen, sms-bommen en voice-respons hebben al bijgedragen aan een daling van het aandeel misbruik oproepen in de periode tot 2009. Met de ingebruikname van de nieuwe 1-1-2 alarmcentrale in 2009 is dit aandeel weer wat gestegen omdat met de nieuwe centrale verbindingen sneller tot stand komen. Na 2010 is de daling weer ingezet. De norm van maximaal 50% onterechte oproepen is echter nog niet gehaald. Het uitsluiten van zogenaamde "simless calls" bleek niet te regelen te zijn via een aanpassing in de Telecomwet. De verwachting is dat via convenanten met de providers komend jaar de daling van het aandeel onterechte oproepen versneld kan worden tot onder de 50%.
- De beschikbaarheid van het alarmnummer is in de periode tot en met 2012 altijd conform norm geweest.

Gesteld kan worden dat, ondanks dat de 50%-norm nog niet is bereikt, de ingezette daling van het aantal onterechte oproepen heeft bijgedragen aan een verbetering van de bereikbaarheid van de alarmcentrale 1-1-2 en daarmee aan een efficiëntere/effectievere communicatie.

4 Beschrijving van de budgetten

Vanwege de structuurwijziging in de begrotingsartikelen per 2010 is dit hoofdstuk opgebouwd uit meerdere paragrafen waarbij onderscheid is gemaakt naar twee perioden: 2007 tot en met 2009 (§4.1) en 2010 tot en met 2012 (§4.3). De eerste periode heeft betrekking op artikel 4.2 (Veiligheidsbeleid op nationaal niveau) en artikel 4.3 (ICT-infrastructuur) en de tweede periode heeft betrekking op artikel 25.2 (Veiligheid, Informatie en Technologie). Tevens is ingegaan op de overgang van de budgetten ten tijde van deze structuurwijziging (§4.2).

4.1 Periode 2007-2009

Vanuit de begroting en jaarrekening is het niet mogelijk om de artikelen 4.2 en 4.3 op te delen naar voor artikel 25.2 relevante onderdelen. Daarom is ervoor gekozen om het financieel verloop over de jaren 2007 tot en met 2009 te baseren op gegevens op programma-/projectniveau vanuit de financiële administratie van MinBZK.

***1.000 euro**	**2007**		**2008**		**2009**	
	Begroting	**Realisatie**	**Begroting**	**Realisatie**	**Begroting**	**Realisatie**
Informatiebeleid	16.652	16.648	14.080	14.537	10.765	9.711
verschil begroting -/- realisatie	*4*		*-457*		*1.053*	
Veiligheid en Technologie – pijler II	-	-	1.000	-	900	160
verschil begroting -/- realisatie	-		*1.000*		*740*	
Veiligheid en Technologie – pijler V	-	-	3.700	899	3.943	3.450
verschil begroting -/- realisatie	-		*2.801*		*493*	
TOTAAL	16.652	16.648	18.780	17.602	15.608	13.321
verschil begroting -/- realisatie	*4*		*3.344*		*2.287*	
relatieve verschil (t.o.v. begrot.)	*< 0,01%*		*18%*		*15%*	

Bron: Financiële administratie MinBZK.

De in 2007 gerealiseerde uitgaven voor de uitvoering van het Informatiebeleid sluit vrijwel exact aan bij het daarvoor begrote bedrag. In de jaren 2008 en 2009 is er echter sprake van een onderuitputting van 15%-18%. Deze is het gevolg geweest van de opstartfase voor het innovatiebeleid waarin dit beleid eerst inhoudelijk en procesmatig moest worden vormgegeven waarna uitgaven zijn achtergebleven bij de beschikbare budgetten.

Capgemini Consulting

4.2 Conversie van begrotingsartikelen 2010

Het artikel 25.2 is in 2010 ontstaan vanuit onderdelen van artikelen 4.2 en 4.3. De delen van artikelen 4.2 en 4.3 die niet naar artikel 25.2 zijn overgegaan, kregen een plaats in respectievelijk artikel 25.1 en artikel 23.3. Uit onderstaande tabel is te concluderen dat de conversie van deze artikelen financieel sluitend is verlopen.

Oude indeling	Budget *1.000 euro			Nieuwe indeling
andere artikelen (2.3, 2.4, 16.3)		7.998	49.827	artikel 25.1
artikel 4.2	51.378	41.829		
		9.549	23.162	artikel 25.2
artikel 4.3	80.145	13.613		
		66.532	361.471	artikel 23.3
andere artikelen (2.2-2.5, 4.6, 16.2-16.4)		294.939		

Bron: Begroting BZK 2010.

De 51,4 miljoen euro voor artikel 4.2 is opgedeeld in 41,8 miljoen ten behoeve van onderwerpen die vallen onder artikel 25.1 en 9,6 miljoen voor onderwerpen die vallen onder artikel 25.2. De 80,1 miljoen euro voor artikel 4.3 is opgedeeld in 66,5 miljoen ten behoeve van onderwerpen die vallen onder artikel 23.3 en 13,6 miljoen voor onderwerpen die vallen onder artikel 25.2. De 9,6 miljoen euro uit artikel 4.2 en de 13,6 miljoen euro uit artikel 4.3, tellen op tot 23,2 miljoen euro voor artikel 25.2.

Na de conversie (met stand 23,162 miljoen euro 2010 voor artikel 25.2) hebben de volgende mutaties zich voorgedaan (bedragen *1.000 euro):

Budget 2010 artikel 25.2 na conversie		23.162
▪ Loon en prijsbijstelling	+ 1.947	
▪ Exploitatie C2000	+10.150	+11.347
▪ Programma Veiligheid	-750	
Budget voor ontwerpbegroting 2010		34.509

Bron: Begroting BZK 2010.

De 23,2 miljoen na de conversie is door loon- en prijsbijstelling, en mutaties voor exploitatie C2000 en het programma veiligheid met een totaal van 11,3 miljoen euro opgehoogd tot 34,5 miljoen euro.

4.3 Periode 2010-2012

In onderstaande tabel is voor de jaren 2010, 2011 en 2012 het budget voor artikel 25.2 weergegeven zoals in de ontwerpbegroting is opgenomen, daarnaast zijn de verschillende mutaties en de gerealiseerde uitgaven weergegeven.

Budget *1.000 euro	**2010**	**2011**	**2012**
Ontwerpbegroting 2010	34.509		
▪ Project Cameratoezicht naar MinJUS	-162		
▪ 1e suppletore begroting 2010	-16.913		
Begroting 2010 na mutaties	17.434		
Gerealiseerde uitgaven 2010	17.429		
Ontwerpbegroting 2011		62.877	
▪ Loon- en prijsbijstelling		-1.918	
▪ Reallocatie MIA-V budgetten naar MinELI		-12.750	
▪ Reallocatie MIA-V budgetten naar MinDEF		-5.750	
▪ Reallocatie binnen begroting MINVenJ		-11.142	
▪ Reallocatie SBIR's Fys.bescherming naar MinELI		-2.287	
▪ Correcties begroting 2010		-216	
▪ Onderuitputting FES (2010)		149	
▪ Begrotingsrapport bp 17 en 18		-10	
Begroting 2011 na mutaties		28.953	
Gerealiseerde uitgaven 2011		26.726	
Ontwerpbegroting 2012			26.744
Gerealiseerde uitgaven 2012			pm
Begroting -/- uitgaven	5	2.227	pm
Relatieve verschil (t.o.v. begroting na mutaties)	< 1%	8%	pm

Bronnen: Begroting BZK 2010, BZK 2011 en VenJ 2012, Jaarrekening BZK 2010 en VenJ 2011.

Het verschil tussen de (uiteindelijke) begroting voor de 2010 en de in dat jaar op dit artikel gerealiseerde uitgaven blijft beperkt tot minder dan 1%. Voor 2011 is het verschil 8% en wordt volledig verklaard vanuit de onderuitputting van verplichtingen die op 2011 betrekking hebben maar niet meer tijdig tot betaling gebracht konden worden. Voor 2012 is nog geen vergelijking mogelijk.

Opgemerkt moet worden dat er een onverklaard maar relatief klein verschil (<1%) is geconstateerd tussen het in de jaarrekening 2011 opgenomen bedrag aan uitgaven (26.726 duizend euro, zie bovenstaande tabel) en het totaal van de ons ter beschikking gestelde gespecificeerde uitgaven in 2011 (26.472 duizend euro).

4.4 Conclusies

Ten aanzien van het financiële / budgettaire aspect concluderen wij dat:

- Het inhoudelijk en procesmatig vormgeven van het Innovatiebeleid heeft tot een onderuitputting van de beschikbare budgetten in 2008 en 2009 geleid van totaal 5,6 miljoen euro;
- De conversie van begrotingsartikelen 4.2 en 4.3 naar 25.2 financieel sluitend is verlopen;
- De uitgaven op artikel 25.2 in de periode 2010 - 2011 op een juiste wijze zijn vastgelegd en betrekking hebben op Veiligheid, Informatie en Technologie.

5 Samenvatting en conclusies

In voorgaande hoofdstukken zijn de operationele beleidsdoelstelling 25.2 en de daarbij behorende beleidsinstrumenten nader toegelicht. Beleidsdoelstelling 25.2 is als volgt geformuleerd: “Het bevorderen van efficiënt en effectief gebruik van communicatie, informatie en technologie door de veiligheidspartners”.

In hoofdstuk 2 is een beschrijving en analyse gegeven van de maatschappelijke context en het probleem dat aanleiding vormde voor deze beleidsdoelstelling. Centraal daarin staat het streven naar meer (bestuurlijke) samenwerking in het veiligheidsdomein, het verbeteren van de informatie-uitwisseling en het streven naar toepassing van innovatieve technologieën. Het ministerie van Veiligheid en Justitie rekende deze problematiek tot haar verantwoordelijkheid op twee niveaus:

- Een stelselverantwoordelijkheid voor het veiligheidsdomein door andere overheden in staat te stellen zo effectief en efficiënt mogelijk de veiligheid te vergroten;
- Een beleidsverantwoordelijkheid voor specifieke veiligheidsdossiers en een aantal systemen die als basisvoorziening dienen binnen het veiligheidsdomein.

In hoofdstuk 3 zijn de beleidsdoelstelling en beleidsinstrumenten beschreven. Vervolgens is op basis van gesprekken met betrokken functionarissen en beschikbare documentatie de realisatie van de beleidsinstrumenten nader toegelicht. Het financieel verloop met betrekking tot beleidsdoelstelling 25.2 over de jaren 2007 tot en met 2012 is beschreven in hoofdstuk 4. Op basis van de inhoudelijke en budgettaire realisatie komt Capgemini Consulting tot de volgende conclusies:

1. *De uitvoering van de beleidsinstrumenten vallende binnen de scope van artikel 25.2 van het ministerie van Veiligheid en Justitie (begroting 2012) hebben bijgedragen aan de realisatie van de beleidsdoelstelling.*

Gesteld kan worden dat alle beleidsinstrumenten het efficiënt en effectief gebruik van communicatie, informatie en technologie hebben bevorderd. Echter, doordat de begrippen ‘*bevorderen*’, ‘*efficiënt*’ en ‘*effectief*’ niet nader zijn geoperationaliseerd in prestatie-indicatoren voor drie instrumenten is het niet vast te stellen in welke mate deze bevordering van ICT heeft plaatsgevonden. Op basis van de beschikbare documentatie en de interviews is voor deze instrumenten wel een plausibele relatie vast te stellen tussen de uitvoering van de beleidsinstrumenten en een aantal resultaten in het veiligheidsdomein:

- De samenwerking tussen partners in het veiligheidsdomein is verbeterd door constante dialoog inzake bestuurlijke afspraken, architectuur en technische standaarden. Deze samenwerking komt tot uiting binnen en tussen de kolommen van het veiligheidsdomein (waaronder IASV, NEC, LCMS en de informatiebeleidsplannen per kolom).
- Het Nationaal Noodnet is vervangen door de Nood Communicatie Voorziening. Met dit crisiscommunicatieplatform is de communicatie tussen de aangesloten vitale sectoren ten tijde van grootschalige ICT uitval geborgd.
- De innovatieprogramma’s hebben geleid tot een veelheid aan nieuwe technologieën (of toepassingen daarvan) in het veiligheidsdomein. Door de criteria en het beoordelingsproces voor de subsidietoekenning is aansluiting bij het overkoepelende doel (bevordering van nieuwe technologieën die breed toepasbaar zijn) geborgd.
- De implementatie van het verdrag van Prüm is, met enige vertraging, in januari 2013 gerealiseerd. Met dit verdrag is een geautomatiseerde uitwisseling van vingerafdrukgegevens tussen lidstaten mogelijk.
- Via een nationale adapter is het Europol Informatie Systeem (EIS) gekoppeld aan de BVO (Basisvoorziening Opsporing) van de KLPD en de (voorheen) politiekorpsen in de regio Midden-

Nederland (Flevoland, Gooi en Vechtstreek en Utrecht). De verdere ontwikkeling is opgeschort tot het gereed komen van Summ-IT als opvolger van BVO binnen de Nationale Politie.

2. De beschikbaarheid en misbruik van het alarmnummer 1-1-2 is verbeterd.

Binnen het beleidsdoelstelling 25.2 zijn alleen voor het beleidsinstrument 'misbruik alarmnummer 1-1-2' prestatie-indicatoren geformuleerd. Hierdoor is het mogelijk om jaarlijks de realisatie voor dit instrument te meten tegen de afgesproken norm.

- De inzet van voice-bommen, sms-bommen en voice-respons hebben al bijgedragen aan een daling van het aandeel misbruik oproepen in de periode tot 2009. Met de ingebruikname van de nieuwe 1-1-2 alarmcentrale in 2009 is dit aandeel weer wat gestegen omdat met de nieuwe centrale verbindingen sneller tot stand komen. Na 2010 is de daling weer ingezet. De norm van maximaal 50% onterechte oproepen is echter nog niet gehaald. Het uitsluiten van zogenaamde "simless calls" bleek niet te regelen te zijn via een aanpassing in de Telecomwet. De verwachting is dat via convenanten met de providers komend jaar de daling van het aandeel onterechte oproepen versneld kan worden tot onder de 50%.
- De beschikbaarheid van het alarmnummer is in de periode tot en met 2012 altijd conform norm geweest.

Gesteld kan worden dat, ondanks dat de 50%-norm nog niet is bereikt, de ingezette daling van het aantal onterechte oproepen heeft bijgedragen aan een verbetering van de bereikbaarheid van de alarmcentrale 1-1-2 en daarmee aan een efficiëntere/effectievere communicatie.

3. Ten aanzien van het budgettaire verloop zijn er geen onvolkomenheden geconstateerd

Zowel op het niveau van de afzonderlijke innovatieprojecten als op het niveau van het beleidsartikel als geheel zijn geen financiële onvolkomenheden geconstateerd. Voor de innovatieprogramma's is deze conclusie gebaseerd op de verplichte accountantscontrole als onderdeel van het subsidiebesluit. Voor de budgettaire ontwikkeling op het niveau van de beleidsdoelstelling is geconstateerd dat:

- Het inhoudelijk en procesmatig vormgeven van het Innovatiebeleid tot een onderuitputting van de beschikbare budgetten in 2008 en 2009 heeft geleid van totaal 5,6 miljoen euro;
- De conversie van begrotingsartikelen 4.2 en 4.3 naar 25.2 financieel sluitend is verlopen;
- De uitgaven op artikel 25.2 in de periode 2010 - 2011 op een juiste wijze zijn vastgelegd en betrekking hebben op Veiligheid, Informatie en Technologie.

Tot slot

Samenvattend kan worden gesteld dat de realisatie van de beleidsinstrumenten behorende bij beleidsartikel 25.2 plausibel hebben bijgedragen aan de realisatie van de beleidsdoelstelling. Door het veelal ontbreken van prestatie-indicatoren op het niveau van de beleidsinstrumenten is het echter niet mogelijk om harde conclusies te trekken. Harde conclusies zijn tevens moeilijk omdat de causaliteit tussen de beleidsinstrumenten en beleidsdoelstelling niet eenduidig is. De realisatie van de beleidsdoelstelling wordt immers mede bepaald door factoren die buiten de directe invloedsfeer van het ministerie liggen.

Bijlage A: Leden van de begeleidingscommissie

Drs. J.C. Boudestijn, Ministerie van Veiligheid en Justitie, NCTV.

Dr. D.E.G. Moolenaar, Ministerie van Veiligheid en Justitie, WODC.

Drs. M.C.M. Schermer Voest, Ministerie van Veiligheid en Justitie, DGPol.

Bijlage B: Geïnterviewde personen

Persoon	Organisatie(onderdeel)
Michiel van der Duin	Ministerie van VenJ, DGPol
Sabine Geerdes	Ministerie van VenJ, NCTV
Erik Kroon	Ministerie van VenJ, NCTV
Jaap Lodder	Ministerie van VenJ, NCTV
Edmée Moojen	Ministerie van VenJ, NCTV
Leo Nieuwenhuizen	Ministerie van VenJ, DGPol
Wilbert Schel	Ministerie van VenJ, DGPol
Dennis Willems	Ministerie van VenJ, DGPol
Niek Willemsen	Ministerie van VenJ, DGPol

Capgemini Consulting

Bijlage C: Bestudeerde documenten

Begrotingen

Begroting Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2007, Tweede Kamer, vergaderjaar 2006–2007, 30 800 hoofdstuk VII, nr. 2

Begroting Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2008, Tweede Kamer, vergaderjaar 2007–2008, 31 200 hoofdstuk VII, nr. 2

Begroting Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2009, Tweede Kamer, vergaderjaar 2008–2009, 31 700 hoofdstuk VII, nr. 2

Begroting Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2010, Tweede Kamer, vergaderjaar 2009–2010, 32 123 hoofdstuk VII, nr. 2

Begroting Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2011, Persexemplaar

Begroting Ministerie van Veiligheid en Justitie 2012, Tweede Kamer, vergaderjaar 2011–2012, 33 000 VI, nr. 2

Jaarverslagen

Jaarverslag en slotwet Binnenlandse Zaken en Koninkrijksrelaties 2007, Tweede Kamer, vergaderjaar 2007–2008, 31 444 VII, nr. 1

Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2008, Tweede Kamer, vergaderjaar 2008–2009, 31 924 VII, nr. 1

Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2009, Tweede Kamer, vergaderjaar 2009–2010, 32 360 VII, nr. 1

Jaarverslag en slotwet Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2010, Tweede Kamer, vergaderjaar 2010–2011, 32 710 VII, nr. 1

Jaarverslag en slotwet Ministerie van Veiligheid en Justitie 2011, Tweede Kamer, vergaderjaar 2011–2012, 33 240 VI, nr. 1

Overige Documenten

ACIR (2005) De vrijblijvendheid voorbij, op naar een effectieve multidisciplinaire informatievoorziening bij grootschalig gezamenlijk optreden in onze gedecentraliseerde eenheidstaat.

Algemene Rekenkamer (2011) ICT bij de Politie, Tweede Kamer, vergaderjaar 2010–2011, 29 350, nr. 9

Algemene Rekenkamer (2012) Prestaties in de strafrechtketen, Tweede Kamer, vergaderjaar 2011–2012, 33 173, nr. 1

Begroting I&IB, 2012-1014

Begroting VIT 2011-2014

Beleidsdoorlichting OD 25.2.doc (eerste opzet gemaakt door VenJ)

Beleidsvisie Veilig door innovatie

Bijlage bij notitie NCTV Innovatiebudget

Capgemini (2008) Toetsingsrapportage Maatschappelijke innovatie agenda's Veiligheid

Capgemini (2008) Verslag ASE Veiligheid

Capgemini Consulting (2010) Analyse voortgang Maatschappelijke Innovatieagenda's

FEZ/FM (2002) BZ-beleid voor de organisatie van de evaluatiefunctie, Doorvertaling van de Regeling Prestatiegegevens en Evaluatieonderzoek Rijksoverheid

Financiën M&ICT-projecten

Hans Lanser (2011) Vervolgstappen zetten, Advies over de landelijke besturing van de informatievoorziening brandweer, In opdracht van de Programmaraad Informatiemanagement van de NVBR

Hans Lanser (2012) Leren vragen, evaluatie van de Brandweer Vraagorganisatie Inhormatiemanagement (BVIM) In opdracht van de Programmaraad Informatiemanagement van de NVBR

Innovatieprogramma veiligheid, Analyse

Maatschappelijke innovatie agenda Veiligheid – advies toekenning middelen

Maatschappelijke Innovatie Agenda's Veiligheid, Factsheet, maart 2009, Nederland ondernemend innovatieland

Maatschappelijke Innovatie Agenda's, Factsheet, maart 2009, Nederland ondernemend innovatieland

Maatschappelijke innovatieagenda Veiligheid, 2008, Nederland Ondernemend Innovatieland

Manifest principes informatiebeleid veiligheid

Meerjarige verplichtingen Pijler V

MIA Veiligheid, Voortgangsverslag over de periode 2009

Ministerie van Algemene Zaken, Samen werken samen leven, Beleidsprogramma Kabinet Balkenende IV

Ministerie van Binnenlandse zaken en Koninkrijksrelaties, Aanbiedingsbrief beleidsdoorlichting artikel 4 uit de BZK-begroting 2006, Tweede Kamer, vergaderjaar 2006–2007, 30 985, nr. 1

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Brief: Niet openbare Europese aanbesteding 1-1-2 centrale mobiele telefonie, dd 5 oktober 2006, Kenmerk 2006-0000157354

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Brief: Nieuwe Infrastructuur mobiele communicatie (c2000) Tweede Kamer, vergaderjaar 2009–2010, 25 124, nr. 64

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Directie politie en Veiligheidsregio's), Nota: Nieuwe werkwijze innovatie dd. 7 januari 2011, Kenmerk: 2011-0000012391

Ministerie van Binnenlandse zaken en Koninkrijksrelaties, Folder Informatie Beleid Veiligheid

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2009) Het informatiebeleid Veiligheid: verbinding in veiligheid, December 2009, Kenmerk B-5571

Ministerie van Binnenlandse zaken en Koninkrijksrelaties (2009) Eindrapportage expertgroep C2000, 22 december 2009

Ministerie van Economische zaken (2008) Aanbieding langetermijnstrategie Nederland Ondernemend Innovatieland en Maatschappelijke innovatieagenda's veiligheid en gezondheid

Ministerie van financiën (2006) Regeling periodiek evaluatieonderzoek en beleidsinformatie 2006, Beleidsdoorlichting artikel 4/Operationele Doelstelling 3, MvT BZK Begroting 2006, TK, vergaderjaar 2005-2006, 30300, hoofdstuk VII nr.2

Ministerie van Financiën (2006) Regeling periodiek evaluatieonderzoek en beleidsinformatie, Beleidsdoorlichting artikel 4/operationele doelstelling 3 BZK 2005, TK, Vergaderjaar 2004-2005, 29800 Hoofdstuk VII nr. 1

Ministerie van Financiën, Regeling Periodiek Evaluatieonderzoek en Beleidsinformatie 2006

Ministerie van Financiën, Rijksbegrotingvoorschriften 2013

Ministerie van Veiligheid en Justitie, Aanbiedingsbrief aanvalsprogramma IV politie 2011-2014, dd. 19 september 2011, Kenmerk: 20110-2000413784

Ministerie van Veiligheid en Justitie (2008) Brief: Informatievoorziening multidisciplinaire ICT projecten in het

Nota Goedkeuring aanbesteding Noodcommunicatie Voorziening, dd 23 juni 2008, Aan: Stuurgroep Nationale Veiligheid, Kenmerk 2008-0000280602

Nota (2007) Nationaal Noodnet, dd 28 november 2007, Aan: het directeurenoverleg Vitaal

Notitie (2010) Inzet budgetten Maatschappelijke sectoren en ICT en Pijler II Middelen voor Maatschappelijke Innovatie Agenda Veiligheid, dd 17 juni 2010

Overzicht van uitgaven VIT 2010-2012

Presentatie Innovatie Veiligheid, Door: Michiel van der Duin

Programmaraad Interdepartementale Programmadirectie Kennis en Innovatie, Verslag vergadering 22 april 2008

Regeringsverklaring Minister-president Rutte, dd. 26 oktober 2010, uitgesproken in de Tweede Kamer

Roadmap Maatschappelijke innovatie agenda Veiligheid, Fysieke bescherming

Roadmap Maatschappelijke innovatie agenda Veiligheid, Opereren in Ketens en Netwerken

Roadmap Maatschappelijke innovatie agenda Veiligheid, Opleiden, Training en Simulatie

SenterNovem, Innovation Intelligence & Coordination (2007) Innovation Intelligence: verkenning Veiligheid, november 2007

Staatscourant nr.: 22199, Regeling van de Minister van Economische Zaken van 18 juli 2009, nr. WJZ/9119524, houdende wijziging van de Subsidieregeling innoveren in verband met het opnemen van een hoofdstuk inzake innovatie voor maatschappelijke veiligheid

Strategiedocument (2008) Noodcommunicatie Voorziening, 23 juni 2008

Veiligheid, Informatie en Techologie (2010) Memo: MIA-V: budget en governance dd. 2 juni 2010

Notitie (2012) Veiligheidsdomein, dd.12 december 2012, Kenmerk: 312140

VIT programma contracten 2001

Concept Regeerakkoord VVD-CDA, (2010) Vrijheid en verantwoordelijkheid, 30 september 2010

Bijlage D: Tien vragen beleidsdoorlichting

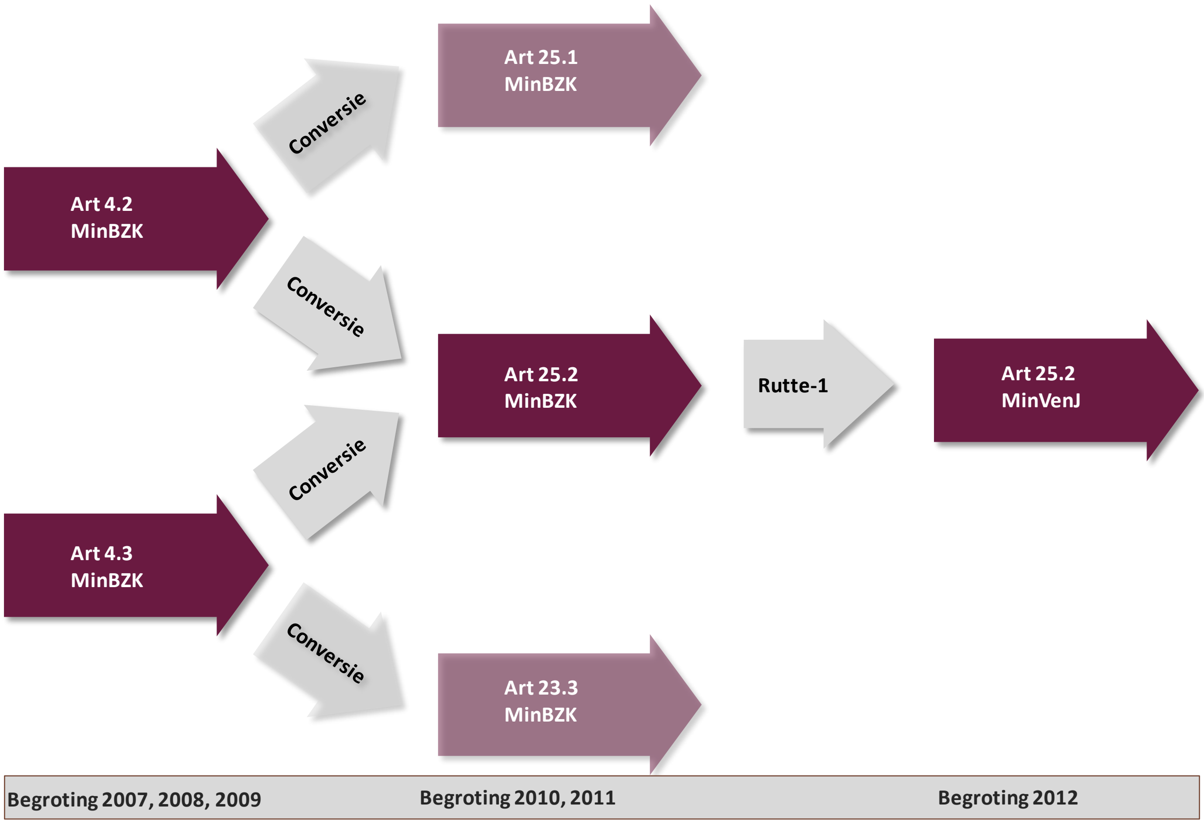
1. Wat is het probleem dat aanleiding is (geweest) voor beleid? Is dit probleem nog actueel?
2. Wat is de oorzaak van het probleem?
3. Waarom rekent de overheid het tot haar verantwoordelijkheid om het probleem op te lossen?
4. Waarom ligt de verantwoordelijkheid op rijksniveau (en niet op decentraal of EU-niveau)? Hoe is de verantwoordelijkheid vormgegeven en waarom?
5. Welke doelstelling heeft de overheid geformuleerd voor de oplossing van het probleem
6. Welke instrumenten (zullen) worden ingezet? Hoe is de samenhang tussen de instrumenten? Is er sprake van verlap?
7. Wat is er bekend over de uitvoering van het beleid en de doelmatigheid van de bedrijfsvoering?
8. Wat was het effect van de instrumenten op de geformuleerde doelstellingen (oplossingen van het probleem)?
9. Hadden de instrumenten op andere beleidsterreinen ook belangrijke effecten op de geformuleerde doelstellingen? Wat waren belangrijke positieve en neveneffecten?
10. Hoe wordt de hoogte bepaald van de budgetten die worden ingezet? Wat is hiervan de onderbouwing?

Bijlage E: Ontstaansgeschiedenis artikel 25.2 MinVenJ

E.1 Inleiding

Het artikel 25.2 in de 2012 begroting van MinVenJ is terug te voeren tot onderdelen van de beleidsartikelen 4.2 en 4.2 in de 2007 begroting van MinBZK. Twee grote gebeurtenissen zijn van belang om te memoreren (zie ook onderstaande figuur):

1. Met ingang van de begroting van 2010 is een nieuwe artikelindeling ingevoerd. Door de nieuwe opeenvolgende nummering van beleidsartikelen is de lezing van de begroting vergemakkelijkt. Daarnaast zijn de beleidsartikelen geactualiseerd om meer informatie te kunnen geven over de kabinetsdoelstellingen waarvoor MinBZK verantwoordelijk is.
2. Met ingang van het eerste kabinet Rutte is het Directoraat-Generaal Veiligheid van het toenmalige ministerie van Binnenlandse Zaken en Koninkrijksrelaties samengevoegd met het ministerie van Justitie. Per 14 oktober 2010 is toen het ministerie van Veiligheid en Justitie ontstaan. Dit heeft voor het eerst zijn weerslag gekregen in de begroting van 2012.



Figuur E.1 Ontstaansgeschiedenis artikel 25.2 VenJ.

In de navolgende paragrafen is ingegaan op de inhoudelijke ontwikkeling van beleidsartikel 25.2.

E.2 Begrotingen 2007 tot en met 2009

Artikel 4.2 en artikel 4.3 maakten onderdeel uit van artikel 4 “Partners in Veiligheid” met als algemene beleidsdoelstelling “Goed samenwerkende partners in Veiligheid”. Naast artikel 4.1 voor apparaatuitgaven en een artikel waar specifieke ontvangsten op werden begroot, bestond artikel 4 uit nog drie artikelen:

Art. 4.2: De bestuurlijke veiligheidspartners ondersteunen met kennis, instrumenten en expertise.

Art. 4.3: Een samenhangende informatiehuishouding van partners in veiligheid.

Art. 4.6: Onderhouden en uitbreiden van internationale veiligheidsrelaties (omschrijving 2007/2008), Onderhouden en uitbreiden van internationale relaties op het gebied van bestuur en veiligheid (2009).

Artikel 4.6 wordt vanaf hier buiten beschouwing gelaten aangezien niets van dit artikel is geconverteerd naar het huidige artikel 25.2. Aangezien de apparaatuitgaven met ingang van de begroting van 2012 in één artikel zijn samengenomen voor het gehele bestuursdepartement, valt ook artikel 4.1 buiten de buiten de scope en verdere beschrijving.

E.2.1 Artikel 4.2: Veiligheid en bestuur

Dit artikel heeft als operationele doelstelling de bestuurlijke veiligheidspartners te ondersteunen met kennis, instrumenten en expertise. Hiervoor zijn in de periode 2007 – 2009 de volgende instrumenten ingezet:

Instrument	2007	2008	2009
Project Veilige gemeente	●	●	
Aanpak verloedering en overlast	●	●	●
Actieplan polarisatie en radicalisering	●	●	●
Actieplan Veilig ondernemen II en III	●	●	●
Centrum voor Criminaliteitspreventie en Veiligheid (CCV)	●	●	
Onderzoeken naar veiligheidsgevoelens burgers	●		
Kennisarena maatschappelijke veiligheid	●		
Veiligheidsmonitor	●	●	
Bestuurlijke aanpak georganiseerde criminaliteit		●	
Monitor criminaliteit bedrijfsleven		●	
Subjectieve Veiligheid		●	
Technologie en Veiligheid		●	
Programma Nationale Veiligheid		●	
Aanpak fietsendiefstal			●
Wetgeving prostitutie			●

Ten behoeve van onderhavige beleidsdoorlichting van art. 25.2 MinVenJ zijn niet alle bovenstaande instrumenten uit art. 4.2 MinBZK relevant. Zie hiervoor de paragraaf E.3 waarin de conversie is toegelicht.

E.2.2 Artikel 4.3: Veiligheid, informatie en technologie

Dit artikel heeft als operationele doelstelling: "een samenhangende informatiehuishouding van de partners in veiligheid". In de periode 2007 – 2009 zijn daarvoor de volgden instrumenten ingezet:

Instrument	2007	2008	2009
Informatie Basisvoorziening/Beleid Veiligheid (IBV)	●	●	●
Eenheid in de informatievoorziening	●	●	
C2000 en GMS	●	●	●
Stimuleren uniforme ICT infrastructuur en informatiehuishouding voor de politie	●	●	●
Samenhangende informatievoorziening voor de brandweer	●	●	●
Samenhangende informatievoorziening voor de GHOR	●	●	●
Actieprogramma maatschappelijke sectoren en ICT	●		
Monitoren implementatie meldpunt fietsendiefstal		●	
Veiligheid en technologie			●
Versnelling verbetering informatievoorziening crisisbeheersing en rampenbestrijding			●
Informatie-uitwisseling tussen Europese rechtshandhaving autoriteiten			●

Ten behoeve van onderhavige beleidsdoorlichting van art. 25.2 MinVenJ zijn niet alle bovenstaande instrumenten uit art. 4.3 MinBZK relevant. Zie hiervoor de paragraaf die de conversie behandelt.

E.3 Begrotingen 2010 en 2011

Zoals reeds vermeld heeft er met ingang van de begroting voor 2010 een herordening plaatsgevonden van de beleidsartikelen. Hierbij is artikel 25.2 (Veiligheid, informatie en technologie (VIT)) ontstaan vanuit onderdelen van artikelen 4.2 en 4.3. De overige onderdelen van deze twee artikelen zijn overgegaan naar respectievelijk artikel 25.1 (Veiligheid en bestuur) en 23.3 (Veiligheidsregio's en politie). In bijlage 8.3 bij de MinBZK begroting voor 2010 is een zogenaamde "is-was artikelindeling" opgenomen. Deze schakeltabel is echter niet opgenomen op het niveau van de instrumenten, waardoor op basis van omschrijvingen van de instrumenten bezien moest worden welke instrumenten van artikel 4.2 en art. 4.3 ook daadwerkelijk zijn over gegaan naar het nieuwe artikel 25.2.

Op basis van die omschrijvingen bleek het echter niet mogelijk om een of meerdere instrumenten uit art. 4.2 aan art. 25.2 te koppelen. Voor art. 4.3 is het wel volledig gelukt om op instrumentniveau de overgang naar art 25.2 en art. 23.3 te maken.

<table>
<tr><th>Art 4.3 instrumenten (voor conversie)</th><th>2007-2009</th><th>2010-2011</th><th>Instrument (na conversie)</th></tr>
<tr><td>Informatie Basisvoorziening/Beleid Veiligheid (IBV)</td><td>●/●/●</td><td>25.2</td><td>Informatie Beleid Veiligheid (IBV)</td></tr>
<tr><td>Eenheid in de informatievoorziening</td><td>●/●/-</td><td colspan="2"></td></tr>
<tr><td>C2000 en GMS</td><td>●/●/●</td><td>23.3</td><td>Beleid infrastructuur en meldkamerdomein, C2000</td></tr>
<tr><td>Stimuleren uniforme ICT infrastructuur en informatiehuishouding voor de politie</td><td>●/●/●</td><td rowspan="2">25.2</td><td rowspan="2">Samenhangende informatie-voorziening voor de brandweer, GHOR en politie</td></tr>
<tr><td>Samenhangende informatievoorziening voor de brandweer</td><td>●/●/●</td></tr>
</table>

Samenhangende informatievoorziening voor de GHOR	●/●/●		
Actieprogramma maatschappelijke sectoren en ICT	●/-/-		
Monitoren implementatie meldpunt fietsendiefstal	-/●/-	Per 2009 ondergracht bij art. 4.2.	
Veiligheid en technologie	-/-/●	25.2	Veilig door Innovatie
Versnelling verbetering informatievoorziening crisisbeheersing en rampenbestrijding	-/-/●	25.2	Invoering netcentrisch werken i.c.m. geografische informatie
Informatie-uitwisseling tussen Europese rechtshandhaving autoriteiten	-/-/●	25.2	Implementatie Europese besluiten en intergouverne-mentele verdragen
Nieuwe instrumenten m.i.v. 2010	}	25.2	1-1-2 misbruik
		25.2	Innovatie en veiligheid voor weerbaarheid tegen terrorisme, criminaliteit en rampen

Artikelen 25.1 en 25.2 vormen samen beleidsartikel 25 met als algemene doelstelling: “een veiliger samenleving door de bestuurlijke kracht van de decentrale overheden en hun partners in veiligheid te versterken”. Artikel 25.1 heeft daarbij als operationele doelstelling “de veiligheidspartners in staat stellen om hun werk efficiënt en effectief uit te kunnen oefenen”. De operationele doelstelling van art. 25.2 luidt “de veiligheidspartners in staat stellen efficiënt en effectief gebruik te maken van informatie en technologie”.

E.4 Begroting 2012

Met de komst van het eerste kabinet Rutte is op 14 oktober 2010 het ministerie van Veiligheid en Justitie ontstaan vanuit het ministerie van Justitie en het Directoraat-Generaal Veiligheid van het toenmalige ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dit heeft voor het eerst in 2012 geleid tot een eigen begroting voor dit nieuwe ministerie. Het beleidsartikel 25.2 is 1-op-1 overgegaan.

Instrumenten	**MinBZK 2010/2011**	**Min VenJ 2012**	***Instrumenten***
Informatie Beleid Veiligheid (IBV)	●/-		Informatie Beleid Veiligheid (IBV)
Samenhangende informatievoorziening voor de brandweer, GHOR en politie	●/●		
Veilig door innovatie	●/-	●	Veilig door innovatie
Invoering netcentrisch werken i.c.m. geografische informatie	●/-		
Implementatie Europese besluiten en intergouvernementele verdragen	●/●	●	Implementatie Europese en internationale verdragen
1-1-2 misbruik	●/-	●	Misbruik 1-1-2 alarmnummer
Innovatie en veiligheid voor weerbaarheid tegen terrorisme, criminaliteit en rampen	●/●		

E.5 Omschrijving operationele doelstelling en motivering van 2012 terug tot 2007

E.5.1 Operationele doelstelling

Begroting	Beleidsartikel	Omschrijving
2012	25.2 MinVenJ	Het bevorderen van efficiënt en effectief gebruik van communicatie, informatie en technologie door de veiligheidspartners.
2011 - 2010	25.2 MinBZK	De veiligheidspartners in staat stellen efficiënt en effectief gebruik te maken van informatie en technologie.
2009 - 2007	4.2 MinBZK	De bestuurlijke veiligheidspartners ondersteunen met kennis, instrumenten en expertise.
	4.3 MinBZK	Een samenhangende informatiehuishouding van de partners in veiligheid.

E.5.2 Motivering

Begroting	Beleidsartikel	Omschrijving
2012	25.2 MinVenJ	Juiste en tijdige communicatie en informatie en toepassing van innovatieve technologieën zijn essentiële randvoorwaarden om het prestatievermogen van de veiligheidspartners en de veiligheid in de samenleving te verhogen.
2011 - 2010	25.2 MinBZK	Informatie en innovatie zijn belangrijke middelen voor de veiligheidspartners om hun presterend vermogen en daarmee de fysieke, sociale en nationale veiligheid van burgers te verbeteren. Door de veiligheidspartners te ondersteunen bij het op orde krijgen van hun informatievoorziening en het stimuleren van innovatieve ontwikkelingen worden zij hiertoe in staat gesteld.
2009 - 2007	4.2 MinBZK	De partners in veiligheid hebben verschillende verantwoordelijkheden in het handhaven van de openbare orde en veiligheid. Een geïntegreerde aanpak van de veiligheidsproblematiek op alle bestuurlijke niveaus is van belang om daadwerkelijk de veiligheid in Nederlands te verbeteren, waardoor de veiligheid en veiligheidsgevoelens in Nederland vergroot worden. Goede samenwerking vereist dat veiligheidspartners goed zijn toegerust om adequaat te kunnen functioneren. Het delen van kennis en expertise zorgt ervoor dat partijen beter presteren en van elkaars ervaringen kunnen leren. Juist op lokaal niveau wordt de veiligheid en het veiligheidsgevoel van de burger bepaald. De gemeenten vervullen hierbij een regierol en worden daarin ondersteund, zoals uit onderstaande instrumenten en activiteiten blijkt.
	4.3 MinBZK	Het is cruciaal dat de juiste persoon op het juiste moment op de juiste plaats over de juiste informatie in de juiste vorm beschikt. De veiligheidspartners dienen bij de uitvoering van de veiligheidstaken de informatie te kunnen uitwisselen door middel van een samenhangend geheel van basisvoorzieningen. De afzonderlijke veiligheidspartners hebben hun eigen informatievoorziening zodanig op orde dat zij de veiligheidstaken op en juiste wijze kunnen uitvoeren.

Capgemini Consulting